Universidade de Aveiro Departamento de Economia, Gestão e Engenharia Industrial
2006

Marco José de Oliveira Pereirinha

Contribuição para o desenvolvimento de um modelo de cartão do munícipe

Universidade de Aveiro
2006
Departamento de Economia, Gestão e Engenharia Industrial

Marco José de Oliveira Pereirinha

Contribuição para o desenvolvimento de um modelo de cartão do munícipe

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Gestão da Informação, realizada sob orientação cientifica do Doutor Luís Manuel Borges Gouveia, Professor Auxiliar da Faculdade de Ciência e Tecnologia da Universidade Fernando Pessoa.

À Cláudia, aos meus Pais e ao meu irmão.

o júri

presidente	Doutor **Carlos Manuel dos Santos Ferreira**, Professor Associado com Agregação da Universidade de Aveiro
vogais	Doutor **José Afonso Moreno Bulas Cruz**, Professor Catedrático da Universidade de Trás-os-Montes e Alto Douro
	Doutor **Luís Manuel Borges Gouveia**, Professor Auxiliar da Faculdade de Ciência e Tecnologia da Universidade Fernando Pessoa (Orientador)

agradecimentos

Agradeço ao Professor Luís Gouveia pela presença e motivação que dedicou em todos os momentos, em especial nos mais difíceis. Pelos seus conselhos e orientações que contribuíram para a presente dissertação.

Agradeço ao Dr. Mário Costa, à Dra. Rossana Fernandes e ao Eng. Paulo Marques pelas preciosas entrevistas que concederam e que serviram de suporte em momentos chave da dissertação.

Uma palavra especial para os colaboradores da JPereirinha que sempre souberam minimizar a ausência do meu contributo para com esta empresa.

Ao Dr. António Salavessa pelas ideias que fomentou.

Aos meus pais que compreenderam os momentos mais críticos e incentivaram a continuação dos trabalhos.

À Cláudia que respeitou a esfera pessoal e que prestou um enorme contributo na revisão dos textos.

palavras-chave

Sociedade da Informação, Gestão da Informação, identificação individual, local e-Government, serviços públicos.

resumo

Uma das principais prioridades da Sociedade da Informação é agilizar os processos burocráticos dos Governos e da Administração Pública. Os governos locais são a fonte de contacto mais próxima das comunidades, apresentando-se como cenário ideal para o desenvolvimento de iniciativas no sentido de apresentar melhorias apreciáveis e contínuas nos seus serviços. A Gestão da Informação neste contexto fruiu das enormes vantagens proporcionadas pelos novos paradigmas tecnológicos. As oportunidades são inúmeras. Todavia, é o conjunto de esforços centrados na integração de informação em áreas limitadas e complementares que permite alcançar resultados.

O presente trabalho pretende prestar um contributo para esse fim. São caracterizadas as necessidades de informação, centradas no munícipe, para uma gestão da informação integrada no contexto do governo local. Para tal, a identificação do munícipe assume um papel crítico.

Partindo de análises críticas realizadas em casos de estudo, onde os dominantes comuns são a identificação e a autenticação de indivíduos, pretende-se contribuir para o desenvolvimento de um modelo para a gestão da identificação do munícipe no contexto do governo local.

O resultado atingido é a apresentação de um estudo que permite considerar a identificação individual como um instrumento estratégico. O objectivo é discutir os aspectos essenciais que devem nortear o desenvolvimento e implementação de sistemas de identificação individual no contexto municipal, levando em consideração as particularidades do contexto nacional – estando, todavia, alinhado com directivas comunitárias, no sentido de num futuro próximo estar inserido num sistema pan-Europeu de identificação dos cidadãos.

keywords

Information Society; Information Management; individual identification; local e-Government; public services.

abstract

One of the main priorities of the Information Society is to speed up the Government and Public Administration's bureaucratic process. The local governments are the closest contact resources of the communities. So, they are considered an ideal scenery for the development of initiatives, in order to provide improved and permanent services. On this context, the Information Management has enjoyed from the huge advantages propitiated by the new technology's paradigms. And the opportunities are countless. However, it is the ensemble of efforts centred on limited and complementary areas that allows great achievements.

This work was done in order to help on this purpose. The information needs, which are centred on the citizen, are characterized by the information transversal management on the local government context. Therefore, the citizen identification assumes an important role.

Beginning with the critical analysis made on study cases, where the common dominant are the individual's identification and authenticity, it is aspired to build a conceptual model to the identification management in a local government context.

The result is the presentation of a study, which allows seeing the individual identification as a strategic instrument. The main porpoise is to discuss the essential aspects that should orientate the development and implementation of the individual identification systems on the municipal context, taking in consideration the particularities of the Portuguese case – being, nevertheless, aligned with the European directives, so that in a neat future it would be inserted on a pan-European system of citizens identification.

ÍNDICE GERAL

ÍNDICE FIGURAS

1 INTRODUÇÃO

Uma das principais razões de sucesso de uma empresa encontra-se no facto desta ter conhecimentos profundos e privilegiados sobre os seus clientes. As informações que as empresas recolhem das interacções com os seus clientes – sejam elas resultantes, por exemplo de *call centers*, processos produtivos, fluxos financeiros, ou outros meios – são processadas e disponibilizadas segundo critérios de gestão da informação institucional. Os colaboradores das empresas que utilizam as informações disponíveis, baseados nos seus valores, crenças e necessidades, podem transformar essas informações em conhecimento. Quanto mais eficaz e eficiente for realizada a gestão da informação adquirida por uma empresa, maior será a vantagem comercial que esta terá sobre uma outra que não o faça tão bem. Pode-se mesmo afirmar que, mais do que um recurso, a informação é um valor. De acordo com João Bilhim (2004), é no espaço virtual que as grandes empresas centram os seus esforços, no sentido de obter maior economia, eficácia e eficiência na gestão da informação.

De forma análoga, o sector público tem cada vez mais a necessidade de conhecer os seus "clientes" – o equivalente ao termo cliente no sector público é cidadão/munícipe. Enquanto que o termo cidadão está associado aos indivíduos que ocupam o território nacional no sentido lato, já o termo munícipe remete para uma maior precisão de localização do indivíduo. Assim sendo, os limites territoriais em que este último se insere designam-se por municípios.

Muitos se questionam acerca da eventual validade da relação entre os binómios empresa/cliente e município/munícipe. A interpretação que é aqui defendida é de que realmente há uma relação directa. Os princípios são os mesmos, i.e., satisfazer as necessidades e expectativas dos seus públicos, de forma a garantir a sustentabilidade. A diferença reside precisamente na fonte de rendimento. Se no sector privado, as receitas advêm directamente dos resultados conseguidos junto dos clientes, já no sector público as receitas resultam das verbas provenientes dos impostos directos e receitas tributárias próprias[1]. Os impostos directos, ou seja, o IRS, o IRC e o IVA, são fonte de 30,5% das receitas[2].

1.1. CONTEXTO E OBJECTIVOS DO TRABALHO

O objectivo principal deste trabalho é contribuir para a proposta de um modelo de gestão da informação autárquica – eficaz e eficiente –, baseado na gestão da identificação individual do munícipe.

Um dos aspectos relevantes é perceber que características, procedimentos, comportamentos, ou até mesmo tecnologias, podem ser incorporadas no sector público – observando por vezes, casos práticos do sector privado, que pela sua natureza competitiva se colocam em elevados patamares de inovação – que poderão conduzir a melhoramentos significativos na gestão da administração pública e do governo local, optimizando, assim, as interacções com os munícipes.

---

[1] Artigo 254.º da Constituição da República

[2] Artigo 10.º da Lei das Finanças Locais

Esta abordagem pressupõe o estudo da operacionalidade do modelo, de modo a aferir os riscos e benefícios que dele poderão advir. O contributo relaciona tecnologias, entidades envolvidas com o município e as pessoas, assim como a autarquia em que se insere.

Tendo em consideração os limites a que estão sujeitos os modelos – devido às suas características intrínsecas e ao elevado grau de abstracção – pretende-se apresentar uma plataforma, que funcione como referencial no desenvolvimento e implementação de soluções ajustadas às especificidades de cada autarquia.

As vertentes digitais do governo e da administração pública, encerram em si inúmeras oportunidades. Como espaços de trabalho, proporcionam contextos onde podem ser desenvolvidas actividades académicas de investigação. Esta conjuntura, aliada à experiência passada do proponente, "O sistema do cartão do cidadão: um contributo para a desburocratização" – projecto final de licenciatura – afigura-se como o cenário ideal de forma a desenvolver o seu trabalho de estudo das necessidades de informação centradas no cidadão/munícipe, considerado neste trabalho como, condição garante última que justifica os princípios dos serviços públicos.

1.2. O CIDADÃO E O GOVERNO ELECTRÓNICO

A participação efectiva dos cidadãos em questões de interesse público exige uma plataforma comum de tomada de decisões. Esta plataforma deverá garantir a compreensão dos temas discutidos – aumentando o rácio qualitativo das informações disponíveis e permitindo um acesso mais fácil e rápido à informação que servirá de suporte à tomada da decisão – assim como a igualdade de tratamento, quer na expressão da opinião individual, quer no direito de voto. Todas estas valências deverão estar claramente aprazadas.

É hoje amplamente aceite o facto das TIC facilitarem a participação dos munícipes. João Bilhim (2004, p.51) refere mesmo que "*as novas formas electrónicas de gestão de informação representam uma oportunidade para incrementar a participação política e a comunicação horizontal entre os cidadãos.*" A

adopção das TIC nas estruturas do Estado e da Administração Pública, conduz estas à condição de governo electrónico.

Por sua vez, André Alves (2004, p.8) advoga que "*o conceito de governo electrónico vai além da incorporação das TIC e inclui também, com crescente relevâncias, a satisfação de exigências para uma Administração Pública menos burocratizada e mais centrada nos cidadãos*". Este autor sintetiza, de forma clara, importantes melhorias relacionadas com a aplicação das TIC – se correctamente implementadas – aliadas à modernização da Administração Pública, no contexto do governo electrónico:

- Desburocratização na prestação de serviços aos cidadão e empresas, com especial relevo na gestão documental e processamento da informação;
- Incremento na rapidez e facilidade de obtenção de informação, logo no esclarecimento de dúvidas dos cidadãos e empresas relacionadas com a Administração Pública;
- Elevação dos padrões de eficiência e redução de custos, com potencial eliminação de níveis mais baixos de gestão e integração de sistemas e serviços sempre que possível;
- Aumento da capacidade de resposta por parte da Administração Pública, potenciando a participação dos cidadãos na democracia de forma mais activa;
- Aproximação dos diferentes vectores da Administração Pública, eliminando a redundância de informação, optimizando os recursos e promovendo a eficaz aplicação do princípio da subsidiariedade.

O momento é propício para salvaguardar que estas melhorias não são taxativas. Atendendo ao facto de estarmos a falar de tecnologias, poder-se-á correr o risco de assumir que um bom sistema tecnológico, devidamente implementado, trará os resultados previstos de forma sistemática. Contudo, isso não é verdade, na medida em que há uma componente humana – que integra as pessoas e as suas competências – envolvida no sistema. Estas pessoas ajudam a desenvolver o território melhorando a qualidade de vida dos seus habitantes. Portanto, é

imperioso que a inovação tecnológica seja acompanhada da adaptação dos processos e das pessoas, pois só desta forma será possível atingir os níveis mais elevados de desenvolvimento do governo electrónico, o estádio Significativo na terminologia da ONU, citada por André Alves (2004, p.11).

Luís Gouveia (2004, p.17) partilhando da mesma opinião, afirma que "*o alvo do e-government não devem ser as tecnologias de informação e comunicação, mas sim o seu uso que, combinado com mudanças organizacionais e novas competências, melhora a prestação de serviços públicos, as políticas públicas e o próprio exercício da democracia...*". Nesta afirmação nota-se de facto, uma descentralização do valor das tecnologias em favor das pessoas. Por muito eficazes e eficientes que sejam as TIC, sem a criação de valor, proporcionada pela acção do Homem através das suas competências, de nada vale a incorporação das mesmas.

A Sociedade da Informação caracteriza-se pelo recurso à informação digital, utilizando para isso as TIC. Esta condição provoca alterações profundas nos hábitos e atitudes implantados na sociedade. As novas formas de trabalhar a informação – propostas pela Sociedade da Informação – têm impacto na produtividade, no potencial económico, na inovação e na maior integração do indivíduo, do grupo e da comunidade, conforme referido por Luís Gouveia e Joaquim Gouveia (2003, p.188).

O desenvolvimento e implementação deste tipo de tecnologias, deve observar as características próprias do modelo de governação adoptado pelas autarquias e ajustar-se a estas. Um modelo eficaz e eficiente numa autarquia, poderá não o ser num outro território. Ainda que considerados como uma referência, estes deverão estar devidamente enquadrados com o governo e a Administração Pública local, assim como com os munícipes.

1.2.1. Os governos electrónicos

Existem diversos conceitos originários do governo electrónico (*e-government* ou simplesmente *e-gov*). Estas derivações resultam em larga medida do factor proxémico em relação ao cidadão. Assim, na sua versão local, o governo electrónico assume-se como *local e-government* – um termo para a qual não foi encontrado o

correspondente em Português – sendo em tudo semelhante ao *e-gov*, ou seja, suporta novos procedimentos de realização das tarefas do Estado e da Administração Pública. Contudo, nesta óptica, o cidadão assume um novo perfil, como já referido, é reconhecido como munícipe.

Num nível ainda mais localizado encontra-se a Autarquia Digital. As suas preocupações estão orientadas para o funcionamento orgânico e quotidiano da autarquia e digitaliza as práticas internas ao recorrer a ferramentas baseadas na Internet. Assim, é possível agilizar e racionalizar os processos. O seu âmbito é interno do poder local e tem como função suportar a infra-estrutura de suporte à decisão autárquica.

No nível mais próximo do munícipe, encontram-se as Cidades Digitais. Ao contrário das autarquias digitais, a questão central aqui é "*fomentar uma maior aproximação entre a administração local, os munícipes, os grandes utilizadores dos serviços autárquicos, as instituições de desenvolvimento regional, as associações de promoção cultural e desportiva, os estabelecimentos de ensino, a indústria, comércio e serviços, os prestadores e utilizadores de serviços de saúde, os turistas e demais visitantes do concelho e todos os que, de uma forma ou de outra, possam ser consumidores de informação, estimulando, paralelamente, o uso das Tecnologias da Informação e Comunicação*", conforme defendem Luís Gouveia e Joaquim Gouveia (2003, p.191). O objectivo fundamental das Cidades Digitais é que as demais partes interessadas na Cidade se envolvam na partilha de informação, permitindo um fluxo de informação livre e garantindo as infra-estruturas necessárias para tal.

1.2.2. As interacções com o governo

As redes de computadores, nomeadamente a Internet, vieram tornar as comunicações mais fáceis. Desta forma, as interacções geradas digitalmente, envolvendo o sector público, podem ocorrer em três níveis distintos. Quando estas ocorrem entre entidades do sector público – Governo ou Administração Pública –, estamos perante o caso *government to government* (G2G). As interacções geradas

entre os cidadãos – onde se inclui a democracia participativa[3] – e o Governo ou Administração Pública, materializam o *government to citizen* (G2C). Existe um outro nível, o *government to employee* (G2E), que engloba as interacções geradas entre os funcionários públicos e os responsáveis por cargos políticos. Este último caso está orientado para a comunicação interna e intimamente ligado à gestão dos recursos humanos.

1.3. CARACTERIZAÇÃO DO CONTEXTO A EXPLORAR

Diversos investigadores têm-se dedicado ao estudo do factor cognitivo de compreensão. A sua definição tem-se revelado uma tarefa difícil. Um caso paradigmático é Nathan Sherdroff (2001, p.27) que a refere como sendo um processo evolutivo e contínuo que medeia os limites Dados e Sabedoria. Para ele, não é simples perceber nem definir as diferenças entre as etapas. A Compreensão pressupõe uma apropriação de tal forma individual, que se torna difícil partilhá-la com terceiros.

Por conseguinte, dados e Informação são termos nem sempre usados da forma mais correcta. De facto, a Informação inclui em si mais valor, logo requer um maior esforço na sua criação e comunicação.

A Figura 1-1, adaptada de Sherdroff, apresenta de uma forma sistemática as relações entre os diferentes estados da compreensão, bem como as principais características de cada uma dessas fases.

[3] O tema democracia participativa será adiante explorado em maior detalhe

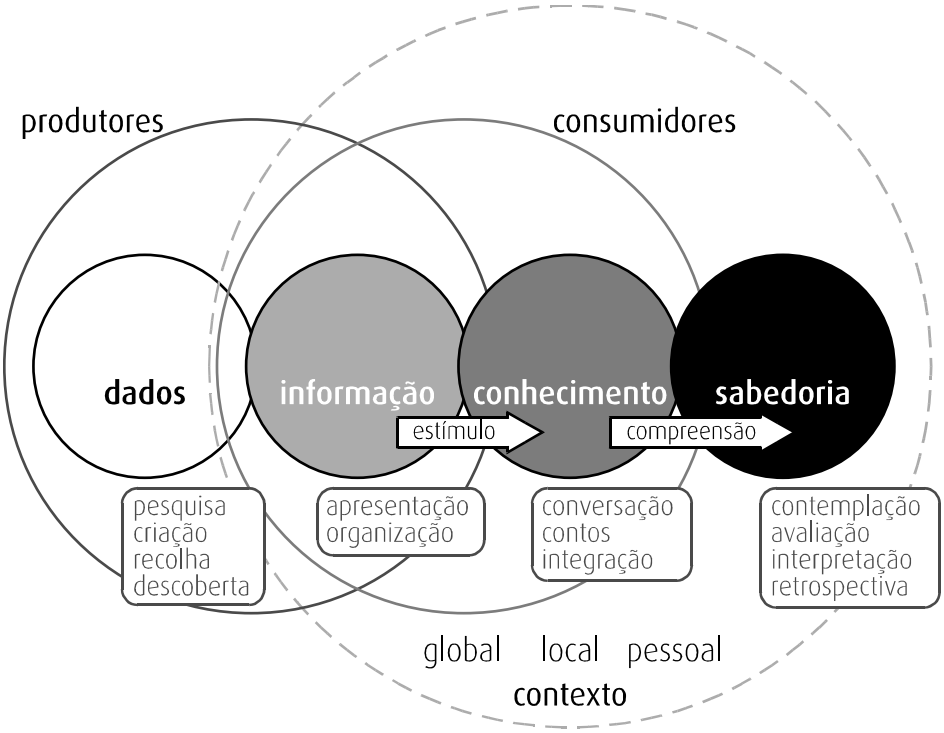

Figura 1-1 – Evolução da compreensão

DADOS

As fronteiras entre dados e informação podem gerar alguma confusão. Contudo, há um factor que define essas fronteiras: o contexto. Sem o contexto, a informação não existe. Alguém disse um dia, "se não informa, não pode ser informação". Pela sua natureza discreta e ausente de contexto, os dados não têm capacidade de informar. Estão normalmente envolvidas nos dados, acções como pesquisa, criação e descoberta.

INFORMAÇÃO

A informação distingue-se pelo seu contexto – condição essencial de valor e de utilidade. Assim, a informação é uma peça essencial no apoio à tomada de decisão. As acções inerentes à informação remetem para a organização e apresentação.

Sherdroff afirma que a informação resulta de arranjos efectuados sobre dados apresentados de diversas formas. Esta manipulação implícita leva a crer que a informação, ao contrário do que se possa imaginar, não é objectiva.

De forma semelhante aos dados, também a informação existe no espaço exterior do indivíduo, ou seja, existe sem este.

CONHECIMENTO

A grande diferença entre a informação e o conhecimento reside na complexidade da experiência necessária para comunicar. Esta é conseguida através da experiência continuada e de diferentes perspectivas do assunto, resultante, em larga medida, da troca de experiências entre pessoas, ou seja, de estímulos exteriores. O conhecimento é algo pessoal e de difícil comunicação.

O conhecimento envolve acções como conversação, conto de histórias e integração.

SABEDORIA

O último estádio da compreensão, a sabedoria, permite aplicar os referenciais adquiridos ao longo do tempo – já pertencentes ao domínio pessoal –, de forma eficaz, em situações completamente novas. Também a contemplação, a avaliação, a interpretação e a retrospecção são consequências resultantes deste momento.

De forma semelhante ao conhecimento, a sabedoria pertence à esfera pessoal, algo que reside no indivíduo, logo difícil de transmitir a terceiros. O seu elevado grau de complexidade, torna-o inatingível para uma grande parte das pessoas.

1.4. CONCEITOS ASSOCIADOS À GESTÃO DA INFORMAÇÃO

Para Feliz Gouveia (2003, p.157), *"a Gestão da Informação prende-se com os esforços organizacionais relacionados com o valor, o custo, a qualidade, a utilização, a origem, a segurança, a propriedade, a distribuição, a fiabilidade, a adequação, e a pertinência da Informação como suporte da missão e dos objectivos organizacionais."*

No contexto dos governos electrónicos, a Gestão da Informação é essencial, pois tem a virtude de integrar esforços – por norma dispersos – no sentido de coordenar, gerir e antecipar as relações complexas dentro do governo e da Administração Pública. Com o advento da geração digital do governo, este perde espaço temporal para recuperar erros de má gestão de informação, algo que ocorre nos cenários mais tradicionais. Hoje, a informação é disponibilizada e acedida à distância de um *click*, sendo a revisão de eventuais falhas, um problema complexo de solucionar.

Earl (in Gouveia, 2003, p.159) relaciona a Gestão da Informação (GI) com a Gestão de Sistemas de Informação (GSI) e a Gestão das Tecnologias de Informação (GTI), como sendo a base duma pirâmide onde o topo é a Gestão Estratégica das Organizações (GE).

A relação obtida deve-se à complementaridade das partes. Assim, enquanto que a Gestão da Informação se preocupa em responder a "Quem?", a Gestão de Sistemas de Informação responde a "O quê?", a Gestão de Tecnologias de Informação responde à questão "Como?" e, por fim, a Gestão Estratégica responde ao "Para quê?". A seguinte figura ilustra as referidas relações.

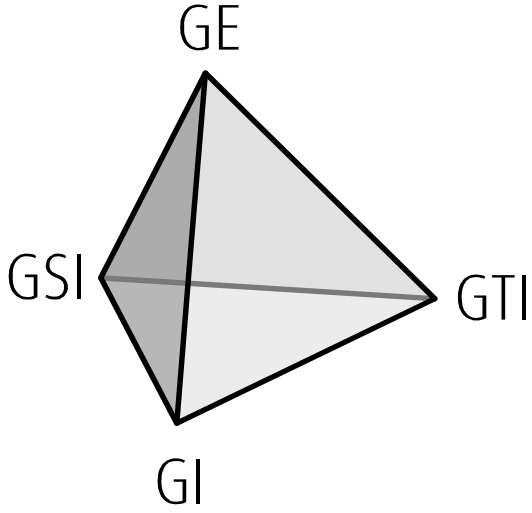

Figura 1-2 – A Gestão da Informação por Earl

1.4.1. Tomada de decisão e as necessidades de informação

Todos os dias somos confrontados com a necessidade de tomar decisões, mas para tal, necessitamos de informação de forma a podermos basear as nossas opções.

Também os gestores, no desenvolvimento das suas actividades e dadas as suas responsabilidades, têm também que tomar decisões. Estes têm que se certificar que dispõem de todos os dados e informação de que necessitam, bem como da qualidade e inteligibilidade dos mesmos.

Segundo Luís Gouveia e João Ranito (2004, p.17), o reconhecimento consciente da inexistência de informação útil para a tomada de determinada decisão levanta uma necessidade de informação. Quando confrontado com uma necessidade de informação, o sujeito deverá em primeira instância verificar a existência da informação necessária. Se existir, deverá tomar posse dessa informação de forma a poder assimilar o seu conteúdo.

1.4.2. Funções e qualidade da informação

Luís Gouveia e João Ranito (2004, p.15) propõem a divisão das funções da informação em 3 grupos:

- Processamento (que inclui tratamento e cruzamento);
- Comunicação;
- Armazenamento.

O tratamento apresenta-se como sendo a função mais simples, resumindo-se à combinação, alteração e manipulação de dados, de forma a produzirem-se novos dados.

Por seu lado, o cruzamento de dados e a informação permite acrescentar valor às partes. Este cruzamento pode realizar-se com dados e informações provenientes de diferentes fontes, numa envolvente de partilha, garantindo a qualidade dos mesmos e as operações de diferentes actores em simultâneo.

Já a comunicação de dados e informação compreende todos os mecanismos associados com a recepção e transmissão destes elementos, onde seja permissível definir quais as origens e os destinos dos mesmos para que seja possível aferir a sua qualidade.

Por fim, o armazenamento é o garante da persistência e manutenção da operacionalidade, para uso posterior, como registo ou como controlo, de dados e de informação. Esta função deverá garantir que os dados e a informação sejam processados e comunicados.

Estas funções determinam o valor, a importância e a qualidade dos dados e da informação. Os mesmos autores apontam um conjunto de quatro características que permitem avaliar a qualidade da informação. Elas são:

- **Precisão**: determina o grau de rigor associado à informação, sendo sinónimo de informação correcta.
- **Oportunidade**: relacionada com o tempo e o espaço do acesso à informação.
- **Completude**: o valor da informação aumenta conforme mais completa ela for.
- **Concisão**: a informação deve ser simples de descodificar e fácil de transmitir. O oposto, o excesso de informação, é análogo à falta de informação.

1.4.3. Fases da Vida da Informação

A Informação experimenta diferentes vivências ao longo do tempo. Importa então perceber quais os estádios pela qual passa e quais as principais características de cada um desses momentos.

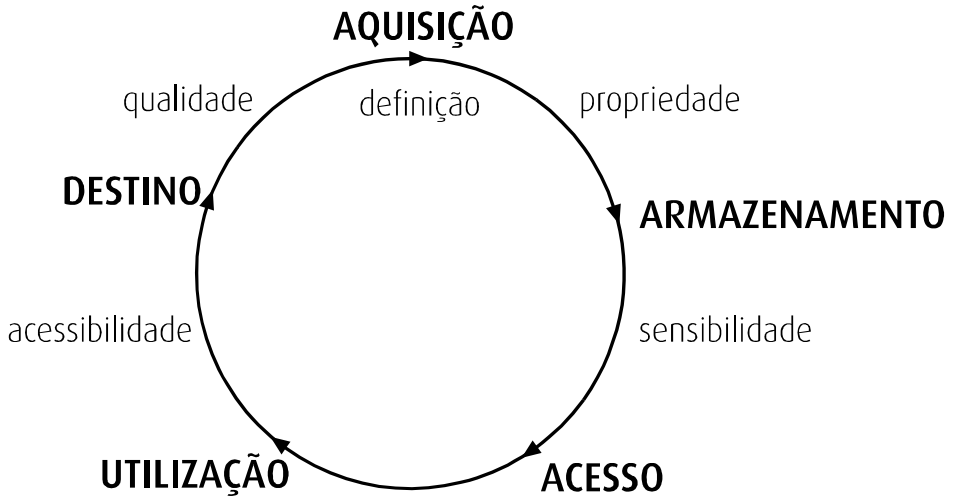

Figura 1-3 – Fases da Vida da Informação[4]

AQUISIÇÃO

Como um recurso que é, a Informação adquirida deve satisfazer os objectivos propostos. A relação custo/benefício deve ser uma das métricas utilizadas neste momento.

A aquisição da Informação pode ser realizada por meios próprios: contratar a sua aquisição ou comprá-la – normalmente existem empresas especializadas fornecedoras de informação em diferentes suportes. Independentemente da forma utilizada na aquisição, devem ser observados critérios de selecção do formato/suporte, de forma a se evitarem desconfortáveis incompatibilidades de sistemas, ou custos adicionais resultantes do tratamento posterior da informação.

ARMAZENAMENTO

No armazenamento da Informação deve-se ter no horizonte a necessidade de partilhar informação respeitando os critérios de confidencialidade definidos na Gestão da Informação. Deve-se ainda ter como principais objectivos a maximização da utilização da informação e a minimização dos custos associados com a sua difusão.

[4] Adaptado de GOUVEIA, Feliz Ribeiro (2003, p.163)

A Informação armazenada deve conter em si as seguintes características: ser precisa, completa, válida, actual, fiável e relevante para as pretensões em causa. No armazenamento deve-se garantir que no acesso, a informação seja disponibilizada num formato compreensível e conveniente para o utilizador. Nestes casos, a qualidade das interfaces de acesso poderão condicionar a interacção homem-máquina.

De forma a satisfazer um acesso rápido e preciso à informação, esta deve estar devidamente catalogada, usando uma taxionomia clara e de uso simples, para que seja facilmente indexada e posteriormente recuperada.

ACESSO

A Informação retornada no acesso deverá estar contextualizada com a necessidade em causa, para que possa surtir os efeitos desejados. O acesso combinado a distintas fontes permite cruzar informações que sejam complementares, gerando valor acrescentado. Isto garante da atribuição, por exemplo de notas pessoais, alterações ou correcções às informações e permite enriquecer as mesmas. Por fim, as possibilidades de partilha da informação e, eventualmente, a capacidade de transformação da informação num outro formato – de forma a ser acessível a terceiros – completam o conjunto de mais valias que se pode esperar nesta fase.

UTILIZAÇÃO

É desejável que a utilização da Informação recolhida se traduza em efeitos práticos no seio da organização, sinónimo de que é útil para os objectivos no momento. Esses efeitos deverão ter um impacto positivo quer na produtividade, quer na eficácia.

Devem ser realizadas auditorias regularmente, a fim de detectar necessidades de informação e aferir a qualidade da informação acedida.

DESTINO

Dependendo do carácter da informação, esta poderá ser arquivada, tendo em consideração critérios de preservação – eventualmente para memória futura –,

salvaguarda, confidencialidade e relevância. Por outro lado, há informação cujo destino é a destruição. Logo, é claramente necessário que o destino a dar à informação esteja devidamente documentado, de forma a se evitarem erros de processo.

Existe Informação de tal modo específica que o destino a dar à mesma está legislado. Logo, é obrigatório ter um comportamento adequado à situação em causa.

1.5. CIDADANIA E PARTICIPAÇÃO

De uma forma geral, a classe política tem perdido a credibilidade que teve no passado. Um sinal claro desta situação é a sistemática elevada percentagem de abstenções, ou votos nulos, que se verificam nas recentes eleições em Portugal – sejam elas autárquicas, legislativas ou até mesmo presidenciais. Como menção, pode-se referir que neste último caso, as presidenciais de 2006 onde, segundo o STAPE[5], cerca de 37% dos eleitores não efectuaram o seu dever de voto.

As sociedades modernas almejam a denominada democracia participativa que se traduz numa partilha de poderes e responsabilidades por parte dos governos para com os seus cidadãos. Para tal, devem ser reforçados os meios de envolvimento público, sendo este processo entendido como um mecanismo que permite potenciar a qualidade das decisões tomadas. Neste caso, a não participação do cidadão é tida como um indicador da sua insatisfação.

Por outro lado, numa perspectiva tradicional a perspectiva é totalmente oposta. A participação é percebida como um sinal da insatisfação dos cidadãos, pelo que é preferível que a sua participação fique apenas pelo momento do voto eleitoral. Importa notar que as formas de gestão adoptadas pelas democracias tradicionais estão normalmente assentes em modelos de liderança gestionária[6].

[5] http://www.stape.pt/eleiref/pr2006.htm

[6] Mais informações em CUNHA, Miguel (2003, p.272) e BILHIM, João (2004a, p.38)

Nesta perspectiva, a participação do cidadão é interpretada pelo sujeito de determinada forma que na prática não se traduz, funcionando apenas como um engodo que visa a sua sedução.

Outros obstáculos que se colocam à democracia participativa estão associados com a morosidade na tomada de decisão – no caso duma participação elevada, há que atender a todos os participantes e discutir todas as ideias. Esta situação poderá ainda conduzir à falta de valor acrescentado da decisão, quando esta já foi amplamente discutida ou quando se prende com situações do quotidiano, ou seja, quando há sobrevalorização de medidas a curto prazo. Há ainda o risco potencial de grupos bem organizados manipularem a negociação e conduzirem a decisão em seu favor.

A participação dos cidadãos conduz à diminuição do valor do *one-man show*, figura central no modelo de democracia representativa, uma vez que no processo de partilha, enquanto uns ganham, outros têm obrigatoriamente que ceder.

Não há pretensão de mudança do estado actual – como referido por João Bilhim (2004, p.62), *"o sistema representativo é o menos mau que se conhece"* – uma vez que, para além do voto, não estão implantados hábitos de participação nos cidadãos portugueses. No cenário actual, parece-nos que, uma vez implementados modelos de governação de tal forma inovadores, estes estariam condenados à nascença por falta de competências criticas dos cidadãos. Assim, há que aplicar medidas no imediato percebendo, com a devida antecedência, que estas apenas surtirão efeitos a médio e longo prazo.

Todavia, e atendendo à complexidade de uma democracia participativa, o seu estado ideal potencia realmente medidas que permitem a satisfação dos munícipes, atribuindo-lhes poderes e responsabilidades, diminuindo a intervenção do poder local. As medidas tomadas estão, assim, mais ajustadas aos interesses das populações. Esta descentralização tem a virtude de desfocar as barreiras entre o público e o privado promovendo, deste modo, o surgir de grupos voluntários de interesse público.

Defende-se, em suma, inovações nos modelos de gestão governamental, centradas na promoção do envolvimento do cidadão aquando da tomada de decisão.

1.6. ORGANIZAÇÃO DO TRABALHO

No **Capítulo 2: Requisitos de Gestão de Informação municipal**, deparam-se as principais expectativas, sob o ponto de vista nacional, mas também ao nível da União Europeia, em relação à sociedade da Informação, mais precisamente o Governo Electrónico. Realçam-se as principais preocupações e estratégias no desenvolvimento de projectos enquadrados nesta temática.

O **Capítulo 3: Sistemas de identificação individual, requisitos associados,** é baseado em esforços desenvolvidos a nível internacional, mas também no contexto que se nos oferece Portugal, aponta um conjunto de condições essenciais a considerar, numa perspectiva de Local e-Government, ao desenrolar de um projecto de identificação de munícipes.

A dissertação assume o expoente máximo no **Capitulo 4: Proposta e discussão de um modelo,** que resulta no contributo para um modelo de inovações profundas nos sistemas de gestão da informação municipal, baseadas na identificação do munícipe, que promovam a desburocratização dos serviços municipais. Por um lado deverá satisfazer os interesses dos munícipes. Por outro, deverá contribuir para o melhoramento do desempenho dos municípios.

O último capítulo apresenta as conclusões mais relevantes do trabalho. Poder-se-á avaliar a satisfação dos objectivos iniciais e apontam-se caminhos para desenvolvimentos ulteriores.

Por fim, são incluídas algumas informações que se julgam pertinentes, sob forma de anexos, dos quais se destacam um conjunto de entrevistas que resultam da participação de representantes da Administração Publica local, do sector bancário e de um empresa que proporciona serviços inovadores. Estes anexos ajudam a completar e reforçar ideias defendidas durante a dissertação.

2 REQUISITOS DE GESTÃO DA INFORMAÇÃO MUNICIPAL

A gestão da informação, no seu sentido lato, tem como objectivo primordial garantir que a informação seja gerida como um recurso indispensável e valioso, bem como assegurar que essa mesma informação está alinhada com os objectivos da organização.

2.1. GOVERNO ELECTRÓNICO

"E-Government promises to deliver better, more efficient public services and improve the relationship between citizens and their governments. The resulting benefits to the quality of life,

industrial competitiveness and society will only be realised, however, if administrations change de way they operate."

eEurope 2005.

Em 2002 a Comissão Europeia definiu o plano de acção eEurope 2005 que, entre outros, determinou estratégias no âmbito do governo electrónico. O factor chave é o recurso às tecnologias de informação e comunicação como integrador das relações entre os governos, empresas e cidadãos. A mudança de paradigma proposta tem em vista as seguintes vantagens:

- Redução de custos quer para o governo, quer para as empresas, diminuindo a carga fiscal e promovendo a competitividade;
- Um sector público mais transparente e propenso à participação dos cidadãos, reforçando a democracia;
- A Administração Pública pode centrar o seu esforço nos cidadãos e na inclusão, disponibilizando os seus serviços 24 horas por dia, 7 dias por semana.

A capacidade de lidar com grandes quantidades de dados e informação que os computadores detêm, aliada à sua capacidade de comunicar em rede global, veio projectar de forma irreversível o governo electrónico, tornando-se no meio privilegiado de comunicação, quer interno, quer externo para um estado moderno.

As metas propostas no plano de acção e-Europe 2005 são as seguintes:

- **Serviços públicos interactivos:** deverá ser garantida a interactividade de serviços básicos, sendo acessível a todos;
- **Pontos de acesso públicos:** serão disponibilizados pontos de acesso públicos com banda larga;
- **Banda larga:** todos os serviços públicos deverão dispor de banda larga;
- **Interoperabilidade:** sempre que possível, deverão ser utilizadas tecnologias que permitam comunicar de forma transversal em todas as autarquias europeias;

- **Cultura e turismo:** deverá ser disponibilizada informação de fácil uso e interpretação promovida pela comissão europeia, pelos estados membros, pelo sector público e pelas autoridades regionais, de forma a atrair a Europa;
- **Comunicações seguras entre serviços públicos:** deverão ser disponibilizadas condições para que se estabeleçam comunicações seguras de informações confidenciais.

O plano de acção e-Europe 2005 encontra-se no fim da sua vida, pelo que a Comissão Europeia lançou o i2010 em sua substituição. Este novo plano, encontra-se ainda numa fase de definição, contudo é de se esperar uma continuidade das directrizes do plano anterior, bem como um aprofundar das exigências. No âmbito do governo electrónico foram já lançados objectivos ambiciosos a serem atingidos até 2010. Estes assentam em 5 pilares essenciais:

- **Nenhum cidadão é deixado para trás**: num claro reforço à inclusão digital, independentemente do género, idade, rendimentos ou deficiências;
- **Aumento da eficiência**: ao empreender no uso das TIC, os governos conseguirão ganhos consideráveis na eficiência e reduções significativas em processos administrativos;
- **Implementação dos contratos públicos electrónicos**: uma grande percentagem dos contratos públicos, deverão ser realizados em linha de forma a reduzirem-se custos;
- **Acesso seguro aos serviços por toda a Europa**: pretende-se que, independentemente do estado membro em que se encontre um cidadão, este poderá aceder em linha aos serviços providenciados pelo seu governo;
- **Incremento da participação e tomada de decisão democrática**: uma consulta pública levada a cabo pela Comissão Europeia, revelou que 65% dos inquiridos acredita que a democracia electrónica conduzirá à redução do défice democrático existente na Europa.

Em Portugal, a UMIC[7] lançou um conjunto de linhas estratégicas destinadas ao desenvolvimento do Governo Electrónico, das quais se destacam:

- Eficiência e facilidade na prestação de serviços ao cidadão com recurso às tecnologias de informação e comunicação;
- Transparência no relacionamento entre o estado e os cidadãos;
- Estabelecimento do balcão único de relacionamento.

Na prática, foi já formado o plano de acção **Ligar Portugal**, integrado no Plano Tecnológico promovido pelo governo português. Ao abrigo deste, a UMIC lançou o **Fórum para a Sociedade da Informação** que pretende assegurar a participação regular de actores relevantes no sentido de desenvolver a Sociedade da Informação.

2.1.1. Inclusão

Mark Poster, citado por Tomás Patrocínio (2003, p.21), afirma de forma explícita que *"foi transporto um limiar, de modo talvez irreversível, no qual a espécie humana procede como nunca antes à difusão destas práticas no seu seio, por mais desigual e assimetricamente que isso possa acontecer"*. Daqui deduz-se que emerge um novo tipo de cidadão que, para além da existência física no território, assume também um papel importante no contexto virtual, sendo identificado como uma única identidade verificando-se assim, a integração entre o real e o virtual.

Em oposição a este tipo de cidadania – onde os munícipes estão preparados e formados para tirar partido das vantagens da Sociedade da Informação – encontra-se a exclusão digital – como propõe André Alves e José Moreira (2004, p.45). Neste grupo estão incluídos os cidadãos com necessidades especiais, assim como todos aqueles sem competências na utilização das TIC.

A Sociedade da Informação deverá satisfazer requisitos físicos, através da facilitação do acesso à tecnologia, ao disponibilizar centros tecnológicos e requisitos

[7] http://www.umic.pt/UMIC/GovernoElectronico/LinhasEstrategicas/

operacionais, onde os fóruns se assumem com principal importância ao servirem de interface entre os munícipes e o governo local. Os centros tecnológicos referidos deverão estar estrategicamente localizados, cujo acesso seja facilitado. Saliente-se o facto dos mesmos estarem orientados para as populações com rendimentos de tal forma baixos, que de outra forma não lhes seria possível aceder a este tipo de recursos. Assim sendo, deve-se providenciar – para além do acesso à tecnologia – formação e apoio, uma vez que há uma provável correlação entre a situação socio-económica e competência em lidar com os sistemas em questão.

Assim, ficam demonstradas as necessidades de autonomia e de independência dos cidadãos com necessidades especiais, assim como a simplificação de processos, a utilização de interfaces simples e a formação daqueles que evidenciam deficiências na utilização das TIC, a fim de tornar a Sociedade da Informação acessível a todos sem quaisquer barreiras socio-económicas.

2.1.2. Participação

> *"A participação directa e activa de homens e mulheres na vida política constitui condição e instrumento fundamental de consolidação do sistema democrático, devendo a lei promover a igualdade no exercício dos direitos cívicos e políticos e a não discriminação em função do sexo no acesso a cargos políticos." in Artigo 109.º (Participação política dos cidadãos) da Constituição da Republica Portuguesa.*

Existem duas correntes que interpretam a participação dos cidadãos de forma distinta. Por um lado, numa perspectiva conservadora, a participação é tida como a manifestação do desagrado perante o governo local. Já uma perspectiva mais moderna, defende que a ausência de participação na vida comunitária é sim um sinal de insatisfação, sendo que é precisamente a participação activa que aumenta o valor das decisões tomadas.

A participação goza das potencialidades inerentes à utilização dos novos modelos de Governo Local Electrónico, permitindo alcançar uma plataforma única na

tomada de decisão. João Bilhim (2004, p.62) propõe que, para que esta plataforma seja isenta, logo legitimamente democrática, deve ajustar-se aos seguintes critérios:

- Participação efectiva;
- Compreensão;
- Igualdade de voto na tomada de decisão;
- Controlo da agenda;
- Carácter compreensivo.

Ainda que utópica esta referência, ela é a viva voz da necessidade de se inovar no actual sistema representativo. Cada vez mais, os políticos devem direccionar a sua atenção àqueles que os elegem, de forma a potenciar decisões mais acertadas de acordo com os interesses dos seus munícipes. Soluções simples como inquéritos de opinião ou painéis de cidadãos permitem uma participação efectiva dos munícipes havendo, assim, um compromisso nas decisões acordadas.

2.1.3. Eficaz e eficiente

O uso das tecnologias de informação e comunicação por parte dos governos locais têm-se manifestado na redução dos processos burocráticos da administração pública, gerando novos cargos de trabalho qualificado, simplificando e uniformizando os processos de tomada de decisão, aumentando a capacidade de resposta – bem como tratamento transversal – às solicitações dos munícipes, entre muitos outros.

Levy (1999) citado por Paulo Silva (2003, p.219) materializa o conceito de substituição, aliás de senso comum. Por um lado o munícipe beneficia da interacção virtual, evitando deslocações físicas aos centros de administração local. Por outro lado, o município, no sentido lato, beneficia ao reduzir tráfego nas suas ruas. Por fim, também a administração é favorecida pois, para além da inserção automática da informação nos sistemas digitais, é eliminado um filtro humano entre o munícipe e o sistema de informação. Assim será mais fácil a imputação de eventuais erros. A tradicional estrutura administrativa hierárquica remete para termos como verticalidade, rigidez, ou dependência. No entanto, no contexto das cidades digitais,

estes termos estão mais orientados para a transversalidade de competências, o relacionamento individual e a fluidez.

Para André Alves (2004, p.8), o recurso às TIC por parte do governo electrónico tem como objectivo principal a obtenção de ganhos de eficácia e eficiência nos diferentes níveis do Estado e da Administração Pública, incluído a administração local. Este crescente interesse tem vindo a ser materializado nos planos estratégicos – associados ao governo electrónico – denominados de *Internal Efficiency and Effectiveness* (IEE).

Esta forma de governação parte do pressuposto que o munícipe irá agradecer a reforma ao trazer-lhe vantagens económicas, eficiência e eficácia nos serviços públicos que lhe serão prestados. Desta forma, o munícipe poderá adquirir uma predisposição acrescida para participar na vida activa da sociedade.

2.2. PAPÉIS E RESPONSABILIDADES

Sendo um dos patamares superiores da gestão estratégica, a Gestão da Informação deverá estar alinhada com os objectivos do governo local. Daqui decorre o imperativo de envolver os decisores ao mais alto nível, de forma a serem definidas as responsabilidades dos utilizadores, assim como a satisfação das necessidades dos mesmos.

A referida definição das responsabilidades deve incluir os cargos e tarefas de cada perfil de utilização. As responsabilidades são acordadas da forma mais clara possível, a fim de eliminar quaisquer incertezas e devem obviamente ser divulgadas. Nesta determinação de papéis, para além do perfil do indivíduo, deverão ser observadas as essências de cada entidade envolvida no sistema, para que os seus requisitos de informação estejam enquadrados com o ciclo de vida da informação. Feliz Gouveia (2003, p.181) apresenta de forma sistemática a estrutura de gestão da informação e responsabilidades associadas.

2.2.1. Gestão de topo

Os líderes e gestores de topo das partes interessadas do sistema, assim como os responsáveis políticos, têm a importante missão de definir o programa para a gestão da informação, nomeadamente o detentor da informação e a guarda da mesma. Assim, são atribuídas responsabilidades e imputabilidades a todos os perfis que colaboram no programa.

Na prática, o departamento informático municipal poderá ser responsável pela guarda da informação, devendo garantir o seu acesso e segurança. Contudo, não lhe poderão ser imputadas responsabilidades no caso de existirem erros de classificação na inserção da informação.

Para o sucesso da gestão da informação, os gestores de topo devem estar envolvidos e comprometidos, apoiando e contribuindo para a sua implementação, incluindo a disponibilização dos recursos humanos, materiais e financeiros.

2.2.2. Gestor da informação

Nomeado pela gestão de topo e a ela reportando directamente – podendo ser-lhe atribuídas outras tarefas dentro da organização – o gestor da informação deve cuidar pela integração na prática da visão estratégica de topo, ajustando a mesma para a sua viabilidade prática. Tal visão inclui a missão, os objectivos e os planos do programa de gestão da informação.

As responsabilidades do gestor da informação são:

- Integrar a gestão da informação no desempenho da organização;
- Gerir transversalmente todos os recursos de informação, independentemente do seu suporte, formato e ciclo de vida;
- Definir, divulgar, implementar práticas, políticas, normas, procedimentos e técnicas;
- Gerir e coordenar fluxos de informação;
- Estabelecer e manter animada a cultura de informação;
- Estabelecer métricas, monitorizar e optimizar a utilização dos recursos de informação;

- Coordenar mudanças de necessidades e requisitos de informação;
- Coordenar programas de formação.

2.2.3. Utilizadores finais

No desenrolar das suas actividades, os utilizadores têm necessidades de informação para tomarem decisões. Estes devem certificar-se de que os dados e a informação de que necessitam estão disponíveis, para além de conter em si qualidade e serem perfeitamente inteligíveis.

Por outro lado, os rigorosos programas de Qualidade e Segurança Informática exigem a definição das responsabilidades dos utilizadores finais. Assim, todos os utilizadores, independentemente do seu nível, são imputáveis pela utilização que fazem dos recursos de informação que criam e processam.

Sendo o grupo mais populoso no contexto da Gestão da Informação, logo potencialmente heterogéneo e fonte de diferentes competências ao nível de utilização de tecnologias de informação e comunicação, os utilizadores finais têm, por vezes, motivações e necessidades diferentes. Reflicta-se no caso dos funcionários públicos e dos munícipes. Feliz Gouveia (2003, p.184) refere um estudo realizado no EUA que demonstra que 65% dos erros de informação estão relacionados com a entrada de dados, sendo imputáveis aos utilizadores finais. Esta situação revela a necessidade de planeamento na formação dos utilizadores, recorrendo, para o efeito, a programas de formação, apresentações e materiais informativos.

2.2.4. Níveis de Responsabilidade

Atendendo aos perfis enunciados, podem ser-lhes atribuídos três níveis de responsabilidades: o nível estratégico, que envolve a gestão de topo, onde a informação é complexa, sendo apropriada para decisões a longo prazo; o nível tácito, que visa locar os recursos assim como o seu controlo, tem um grau inferior de complexidade e adapta-se à gestão de médio prazo; por fim, o nível operacional, associado às tarefas desenvolvidas pelos utilizadores finais, assente no curto prazo, sendo a fonte básica de criação de informação.

2.3. O MUNÍCIPE COMO FACTOR DE CONVERGÊNCIA

Os esforços realizados no âmbito da transferência do processamento da informação do analógico para o digital, bem como as interacções das instituições que ocupam o território – sejam elas públicas ou privadas – devem ter como horizonte o munícipe. Como veremos em maior pormenor no capítulo 3, está fixado na Constituição da Republica que a Administração Publica deve estar estruturada, de modo a evitar a burocratização. Esta directiva encerra em si duas perspectivas. Por um lado, o agilizar dos processos, por outro a facilitação – não no sentido do descuido – das interacções com os munícipes.

Os actuais e exigentes modos de vida condicionam cada vez mais o tempo disponível para as pessoas se deslocarem fisicamente às instalações das organizações. As novas tecnologias vieram trazer novos paradigmas na comunicação, que permitem em larga medida suplantar a insuficiência do tempo. Cada vez mais as pessoas escolhem formas de comunicar mais rápidas que evitem deslocações, contabilizando ainda os custos a isso inerente. Para além do tradicional telefone, novas formas de comunicar destacam-se designadamente, o correio electrónico e outras ferramentas de interface baseadas em tecnologias de Internet, uma vez que permite resolver problemas à distância.

O recurso às novas tecnologias conduz ao inevitável distanciamento pessoal e ao aumento do individualismo. Todavia, as relações têm tendência a aumentar a sua complexidade. Jorge Xavier (2003, p.140) defende que as novas formas de relacionamento requerem obrigatoriamente uma rede mais complexa, capaz de promover uma maior diversidade na comunidade.

O mesmo autor refere a existência de indicadores que mostram que as cidades digitais promovem uma melhoria significativa na relação com o cidadão. O interesse pelo exercício da cidadania é ampliado pela envolvente gerada pelo envolvimento de diferentes entidades públicas e privadas, e também pela ampliação da identificação do cidadão com o território.

2.3.1. CRM vs CzRM

Como já referido no capítulo introdutório, existe um paralelismo entre os binómios empresa/cliente e município/munícipe. A analogia reflecte-se também nas boas práticas utilizadas na gestão dos seus relacionamentos. No caso da gestão de clientes por parte das empresas, é utilizado o CRM (*customer relationship management*). Já para a gestão do relacionamento com munícipes por parte dos municípios existe o CzRM (*citizen relationship management*). Todavia, existem algumas diferenças que serão explanadas em seguida.

O grande objectivo do CRM é ser a interface entre o cliente e a organização de forma transversal a esta, ou seja, reúne informação sobre o cliente em vários departamentos da organização. A Internet contribuiu de forma inquestionável para o sucesso desta tecnologia, ao disponibilizar um novo canal para o auto serviço do cliente, conforme referem Luís Gouveia e João Ranito (2004, p.75).

O CRM encerra em si não só toda a informação conhecida do cliente (identificativa ou demográfica, por exemplo), mas também resumos de encomendas e vendas, assim como os contactos realizados com o *contact center*. Desta forma, este repositório funciona como um recurso que os colaboradores da organização devem utilizar para que o atendimento e o serviço sejam ainda mais personalizados, aumentando, deste modo, a rentabilidade, bem como taxas de satisfação. Nesta perspectiva, o CRM assume-se como um novo perfil, ou seja, uma estratégia de gestão destinada a manter relações profícuas e duradouras (Jorge Xavier, 2003, p.142). Este novo perfil só é possível quando existe real envolvimento dos colaboradores, assim como quando existam interacções com os clientes.

De forma semelhante, o CzRM também se preocupa com a gestão do relacionamento e recorre às mesmas tecnologias. Contudo, Jorge Xavier (2003, p.143) defende que a questão não é assim tão simples. É proposto que sejam consideradas as seguintes questões:

- Ao longo da vida, quantas vezes um munícipe se dirige à sua Câmara Municipal?
- E à Junta de Freguesia?

- Que interacções gera?
- Se existem poucas interacções, porque irão aumentar com o recurso ao digital ou a centros de contacto?
- Que informação sobre o munícipe é recolhida pelo governo local?
- Qual a fonte dessa informação?
- Como é alimentada?

Analisando-as, poder-se-á constatar que existem munícipes que criam poucas interacções com o governo local (Jorge Xavier, 2003). Assim, o interesse de gerir o relacionamento com estes munícipes seria relativo. Porém, e como será demonstrado com maior profundidade no próximo capítulo, os sectores público e privado tendem a aproximarem-se. Desta forma, o cliente e o cidadão, sendo a mesma pessoa física, propendem a assumir a mesma identidade digital. Esta confluência de identidade, entre o cliente e o cidadão, reflexo da aproximação dos sectores público e privado, gera um ambiente favorável ao desenvolvimento comum do CRM e CzRM. As vantagens são evidentes. Por um lado, para o município e para as empresas, a quantidade de informação gerada é maior, mais rica e mais exacta – levantando-se depois problemas associados com o excesso de informação. Por outro lado, os cidadãos/clientes assumem um papel único, desaparecendo critérios e procedimentos meramente burocráticos na identificação dos mesmos.

Ainda que o munícipe não gere muitas interacções percepcionadas pelo município, no seu quotidiano acaba por o fazer. Seja no relacionamento com estruturas e equipamentos, ou no acto de movimentar-se – eventualmente usando transportes públicos – e actuar no território, são informações que à partida são difíceis de contabilizar.

A grande diferença entre o CRM e o CzRM encontra-se na potencial complexidade que este último pode encerrar em si. Enquanto que no CRM o perfil do indivíduo é único, no CzRM – dada a diversidade do âmbito dos distintos departamentos do governo local, bem como das empresas privadas com acesso ao sistema – os requisitos de informação a que a tecnologia deve responder são incomparavelmente superiores.

2.4. ESTRATÉGIAS

Todas as iniciativas têm estratégias associadas e a gestão da informação municipal não é excepção. Luís Gouveia e João Ranito (2004, p.51) propõem um modelo que segmenta a estratégia em três vectores chave, conforme apresentado na Figura 2-1.

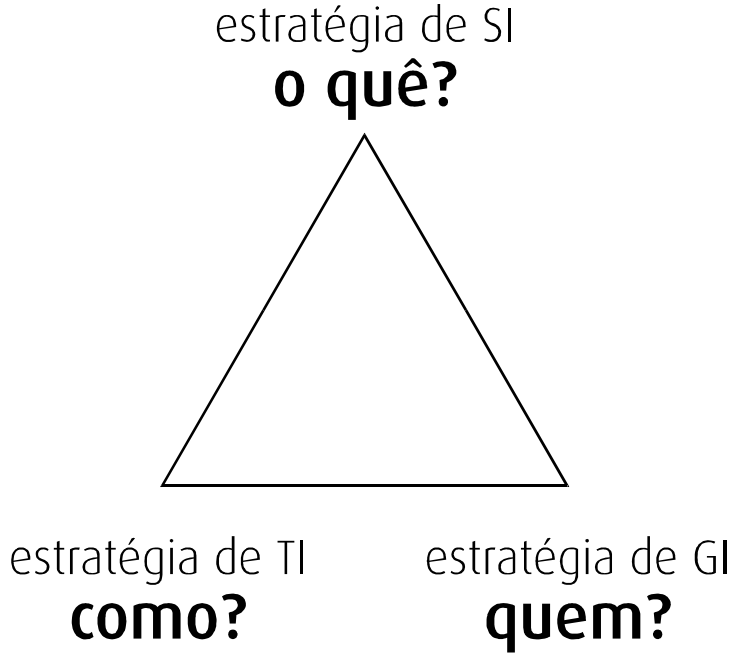

Figura 2-1 Vectores de segmentação estratégica[8]

No vector da estratégia das Tecnologias de Informação (TI), os gestores devem considerar questões relacionadas com o âmbito e arquitectura das TI, por exemplo, o custo, integração ou fornecedores do serviço, respondendo ao "como?".

Por outro lado, o vector estratégico dos Sistemas de Informação explora questões relacionadas com as aplicações e suas funcionalidades. O seu foco é o desenvolvimento da actividade e visa responder ao "o quê?".

Já no vector estratégico da Gestão da Informação, as suas preocupações assentam sobre o ciclo de vida da Informação, sendo neste caso que se definem

[8] Adaptado de Luís Gouveia e João Ranito (2004, p.52)

papeis, responsabilidades e relacionamentos para cada uma das fases. Pelo seu foco na gestão, este vector responde ao "Quem?".

Esta segmentação encerra em si um enorme valor sintético, sendo por isso, adaptada ao tema em estudo na exploração do modelo proposto.

2.5. SUMÁRIO

Este capítulo tratou os requisitos básicos necessários para uma eficaz e fidedigna utilização da informação por parte quer do governo, quer dos munícipes.

É certo que a União Europeia já comprovou as vantagens da implementação de um governo electrónico, como meio primordial de comunicação e de gestão da informação, na medida em que o torna mais eficiente. Isto porque existe uma clara redução de custos e um maior e mais facilitado acesso à informação: trata-se de um balcão aberto 24h por dia, 7 dias por semana ao serviço da população.

Portugal não deve permanecer à margem desta nova tendência europeia. Para tal, torna-se essencial a criação de centros tecnológicos e de fóruns, com vista à ligação entre o governo local e o munícipe. Ora, para que a informação chegue a todos de forma eficaz, é necessário que o governo crie espaços de formação, bem como interfaces de fácil utilização, não descurando os indivíduos com necessidades especiais.

Para o sucesso do governo electrónico, torna-se pertinente que as autarquias invistam nos seus eleitores, de acordo com as suas necessidades e interesses. Logo, deve-se apostar no rigor, na simplicidade, na formação e, sobretudo, na informação, de forma a estreitar os laços entre o cidadão e o governo local. Só assim, será possível fazer com que o munícipe, ou seja, cada um de nós, participe de forma activa na vida de nosso país.

3 SISTEMAS DE IDENTIFICAÇÃO INDIVIDUAL, REQUISITOS ASSOCIADOS

A identificação é um processo através do qual um indivíduo se identifica perante terceiros. Quando recorremos a um departamento governamental, é quase incontornável este processo. Necessitamos de nos identificar perante o funcionário que nos atende recorrendo para tal a certidões, cartões, declarações, num processo burocrático cáustico. Numa sociedade que cada vez mais se afirma como sendo de informação, torna-se premente a mudança de paradigma.

Parte-se do pressuposto consensual que todos os munícipes ambicionam que os seus agentes governamentais locais reduzam a carga burocrática. Assim, parece irrefutável uma simplificação dos processos, de forma que os indivíduos se tornem o centro da atenção dos seus governantes e administradores. Neste enquadramento, a identificação do munícipe é um processo que se requer rápido, em que possam

ser reunidas o maior número possível de informações relevantes sobre o mesmo. Ao mesmo tempo, os munícipes desejam que a sua informação pessoal esteja devidamente protegida ao estar asseverada a segurança dessas informações, estando garantida a sua própria privacidade.

No âmbito do sexto programa quadro comunitário de apoio à investigação e desenvolvimento na temática da sociedade da informação, foram disponibilizadas verbas para projectos que têm como missão explorar a problemática da gestão da identificação dos indivíduos no contexto do governo electrónico. Dos projectos aprovados, destacam-se os consórcios EMAYOR[9] e o GUIDE[10].

O EMAYOR é uma iniciativa que visa desenvolver uma plataforma segura, aberta, interoperacional e ao custo certo para o estabelecimento de comunicações seguras entre pequenas e médias autarquias do panorama europeu, no contexto do local e-Government. Este consórcio dedica especial atenção a questões relacionadas com a autenticação.

Já o projecto GUIDE pretende tornar a Europa líder mundial ao nível dos serviços electrónicos prestados pelos governos membros, através da criação de uma arquitectura aberta para a gestão e autenticação da identificação baseada no relacionamento durável transnacional pan-europeu.

Existem cinco pilares que devem ser considerados pelas organizações que recorram a sistemas de informação usando tecnologias da informação e comunicação, conforme afirmam Luís Gouveia e João Ranito (2004, p.25):

- **Objectivos da organização**: os sistemas de informação devem estar orientados para a satisfação dos objectivos da organização;
- **Hardware**: todo o equipamento físico que permita o processamento, armazenamento e a comunicação;

[9] http://www.emayor.org

[10] http://istrg.som.surrey.ac.uk/projects/guide/

- **Software**: ferramentas lógicas que controlam os hardwares de forma a suportar o desenvolvimento de tarefas;
- **Procedimentos**: envolvem as regras, políticas e comportamentos que permitem atingir os objectivos;
- **Pessoas**: inclui todos os indivíduos, internos ou externos à organização, que de alguma forma e no contexto organizacional possam contribuir para a satisfação dos objectivos.

A fim de serem atingidos os objectivos a que se propõe a gestão da identificação dos munícipes, há um conjunto de requisitos – tecnológicos, operacionais, sociais, legislativos e económicos – que devem ser satisfeitos.

3.1. TECNOLOGIAS E SUA INTEGRAÇÃO

Todos aqueles que baseiam a gestão do seu dia-a-dia em suportes tecnológicos conseguem com alguma facilidade extrapolar as vantagens latentes dessa opção, num contexto organizacional mais alargado, como é o caso do governo local.

Muitos municípios iniciaram já o seu caminho de transformação em *local e-government,* tendo já disponíveis diversas tecnologias que operam em diferentes níveis organizacionais. Luís Gouveia e João Ranito (2004, p.57) sugerem 4 níveis de sistemas de informação: estratégico; gestão; conhecimento; operacional. Analise-se com mais pormenor esta proposta de segmentação.

3.1.1. Tipos de sistemas de informação

NÍVEL OPERACIONAL

Trata-se do nível mais básico de sistema de informação sendo responsável pelo registo de dados resultantes das actividades essenciais da organização. São sistemas que normalmente estão preparados para operar sobre grandes quantidades de dados, pelo que as grandes preocupações no seu desenvolvimento

é a eficácia do desempenho na introdução de dados, relegando para segundo plano a pesquisa.

Os TPS *(Transaction Processing Systems)* ou Sistema de processamento de transacções são um exemplo prático de sistemas de informação ao nível operacional. Estes, são capazes de gerar e armazenar milhões de dados.

A análise em grande escala dos dados armazenados permite fornecer informações essenciais a níveis superiores de decisão, revelando tendências ou oportunidades de melhoria.

NÍVEL CONHECIMENTO

Estes sistemas de informação, como o próprio nome indica, suportam o trabalho daqueles que lidam com o conhecimento, mas também dados. Comportam uma maior flexibilidade do que o anterior nível, devendo permitir o controlo do fluxo de trabalho.

Existem soluções disponíveis no mercado ainda que tenham que ser ajustadas à realidade da organização. Dois casos exemplares são os KWS *(Knowledge Work Systems)* ou Sistemas de Suporte ao Conhecimento e os OAS *(Office Automation Systems)* ou Sistemas de Automação de Escritório.

No primeiro caso, os KWS, ajudam profissionais qualificados na criação e integração de novo conhecimento na organização, como por exemplo as estações de engenharia que permitem os engenheiros definirem o PDM (Plano Director Municipal).

Por seu lado, os OAS, são sistemas que visam incrementar a produtividade do pessoal administrativo, permitindo processar informação, por exemplo, através de processadores de texto ou do correio electrónico.

NÍVEL DE GESTÃO

Os sistemas de informação ao nível de gestão auxiliam a gestão intermédia ao fornecer-lhe informação de controlo e supervisão, que suportam a tomada de decisão numa perspectiva de gestão corrente, operacional e táctica.

Também neste caso, o mercado dispõe de algumas soluções flexíveis que permitem a adaptabilidade às organizações, sendo exemplos práticos os MIS *(Managment Information Systems)*, ou Sistemas de Gestão da Informação, e os DSS *(Decision Suport Systems)*, ou Sistemas de Suporte à Decisão.

Se por um lado, os MIS suportam funções de planeamento e controlo, apresentando sínteses diárias que proporcionam a tomada de decisões estruturadas ou semi-estruturadas, já os DSS, pela combinação de dados e modelos avançados, suportam a tomada de decisão semi-estruturada ou não estruturada. Os DSS ajudam a resolver problemas cujas soluções que não são possíveis de especificar à partida.

NÍVEL ESTRATÉGICO

Os sistemas de informação que satisfazem o nível estratégico estão destinados aos gestores de topo. Estes integram informação multidimensional, proveniente de níveis menos complexos, bem como de diferentes departamentos da organização. Saliente-se o facto do crescendo de complexidade dos níveis, em que no sistema operacional, dados e informação são processados de forma estruturada, e no nível estratégico, o grau de abstracção não permite essa estruturação. Assim, pelo seu carácter volátil, não existem soluções tipificadas no mercado, pelo que normalmente, as organizações optam pelo desenvolvimento interno destas ferramentas.

Os ESS *(Executive Support Systems)* ou Sistemas de Suporte Executivo, suportam a tomada de decisão através de representações gráficas avançadas, exibindo extrapolações a longo prazo de diversos factores chave, como por exemplo, planeamento de curvas de investimento.

A figura 3.1 sintetiza de forma clara o enquadramento dos níveis em relação aos diferentes sistemas de informação, bem como sistematiza o relacionamento entre os esses sistemas.

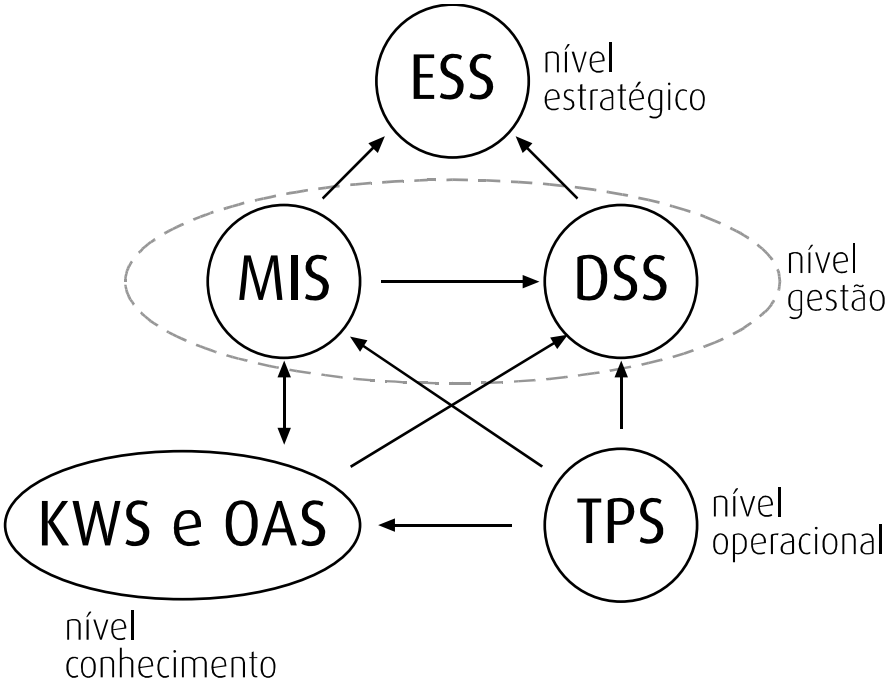

Figura 3-1 Níveis e integração dos sistemas de informação[11]

3.1.2. Outras considerações

A gestão eficaz da identificação do indivíduo poderá ter um papel fundamental na comunicação transversal destes níveis, funcionando como dado integrador. Desta forma, confere-se especial importância a uma perspectiva integradora, não só dos referidos níveis estratégicos, mas também entre entidades públicas e privadas, assim como entre municípios, e entre estes e o governo central. A convergência tecnológica entre as partes interessadas deverá ter em vista a inter operacionalidade, onde a identificação do munícipe é elementar. Contudo, o contexto actual é propício para que o cenário não seja tão linear. Diferentes departamentos e diferentes organismos propendem a ter os seus próprios padrões tecnológicos e terminológicos. Deverá haver então um esforço orquestrado e

[11] Adaptado de Luís Gouveia e João Ranito (2004, p.64)

acordado – devendo evitar a tendência de conservação de soluções existentes de uma das partes – de forma a harmonizar terminologias e tecnologias.

As partes interessadas deverão dispor de tecnologias que permitam reconhecer os instrumentos de identificação do cidadão. Estas não são mais do que terminais com capacidade de interpretar informação constante num suporte digital de informação – por exemplo: smart cards –, ou por outro lado processar características físicas do individuo – a designada biometria – e associar a uma entidade única. Em qualquer dos casos, as maiores preocupações deverão ser a segurança e a privacidade da informação pessoal. A melhor forma de garantir estes requisitos será recorrer a soluções que tenham já maturidade de mercado, e que de preferência sejam normalizadas, como é o caso da linguagem orientada aos objectos JAVA, os sistemas de gestão de base de dados da ORACLE, ou os cartões *smart cards* na identificação individual. Desta forma, evitam-se perdas – de tempo e dinheiro – em investigação e desenvolvimento, fruindo ainda da experiência acumulada resultante dos factores concorrenciais de mercado.

As interfaces entre os sistemas e as pessoas deverão ser simples, intuitivas e amigáveis, em especial quando se tratam de munícipes com aversão à tecnologia na expectativa de os mobilizar para que uma taxa de acolhimento satisfatória seja atingida o mais rapidamente possível.

3.2. REQUISITOS ESTRATÉGICOS E OPERACIONAIS

Os requisitos operacionais estão intimamente ligados com o ciclo de vida da informação, que de forma continuada e sustentada, regenera-se de tempos a tempos com a finalidade de:

- **Avaliar continuamente** das necessidades de informação;
- **Identificar novas oportunidades** de integração e inter operacionalidade;
- Efectuar a **manutenção dos modelos de dados e de processos** da informação;

- Efectuar a **manutenção das normas para os dados e representações** de processos na organização.

Os políticos, administradores públicos e privados, ou seja, as partes interessadas, deverão estar envolvidos e comprometidos na definição estratégica do modelo a adoptar no sistema para a gestão da identificação dos munícipes. Conforme referido no capítulo 2, estas chefias de topo devem ser os promotores dos programas, apoiando e contribuindo através da definição dos perfis e responsabilidades dos utilizadores dos sistemas, bem como disponibilizando os recursos técnicos e financeiros para o desenvolvimento e implementação do sistema.

Os novos papéis desempenhados pelos agentes da Administração Pública devem estar devidamente formatados para potenciar o uso e rentabilização das TIC. O factor humano assume um carácter fundamental no modo como são adoptados os alinhamentos estruturais e procedimentais no seio do seu departamento/instituição. Características como flexibilidade, autonomia e formação – conforme defendem André Alves e José Moreira (2004, p.13) –, são essenciais no desempenho das funções dos agentes da Administração Pública. A flexibilidade pela procura crescente dos ambientes dinâmicos, onde há uma rápida mudança de paradigmas, é uma característica que estimula o desenvolvimento de estruturas menos hierarquizadas, logo menos rígidas. Daqui decorre a autonomização dos indivíduos. Esta condição revela-se como a melhor forma de adoptar processos mais eficientes e de promover a cooperação entre as estruturas. O *empowerment*[12] fomenta a procura incessante em busca da auto eficácia e auto valorização do indivíduo, pois é-lhe induzida a sensação de liderança na prossecução das tarefas que lhe são afectadas. Contudo, sem o esforço e o investimento na promoção da formação e qualificação dos agentes da Administração Pública, os restantes requisitos operacionais associados a estes tendem a ser ineficazes. Para além do aumento da capacidade de utilização eficaz das TIC e da reconversão profissional dos agentes, deverão ser desenvolvidas competências críticas de adaptação à

[12] Mais informações em REGO, Arménio e CUNHA, Manuel Pina (2003, p.149)

mudança, avaliação do desempenho dos serviços públicos e novas formas de agir sobre os mesmos. Ou seja, ser capaz de analisar criticamente a sua envolvente e de tomar medidas no sentido de optimizar o desempenho.

Numa outra perspectiva, vários autores, como é o caso de Ricardo Pinto (2003, p.96), defendem que as mudanças actuantes sobre a forma como as pessoas pensam e comunicam traz maiores resultados quando efectuadas numa estratégia de baixo para cima, ao contrário da imposição superior. Os projectos pioneiros de democracia electrónica revelaram que os decretos, por si só, não são capazes de alterar os modelos de comunicação das pessoas. É importante consciencializar os agentes acerca dos benefícios proporcionados pela mudança, através do contacto directo com a fase de desenvolvimento, ajustando o sistema às necessidades dos utilizadores.

A importância da Informação no contexto organizacional é tal que a sua gestão eficaz é um requisito do programa de Qualidade, nomeadamente da norma ISO 9000, sendo que a existência duma falha no ciclo de vida da Informação compromete o programa de qualidade. Segundo Feliz Gouveia (2003, p.150), na política de Gestão da Informação, existem 3 aspectos fundamentais: a **confidencialidade**, que estabelece a autorização de acesso à informação; a **integridade**, que garante a modificação apenas quando há autorização; e a **disponibilidade**, que acautela o acesso à informação pretendida e quando pretendida. Estes critérios são processados num programa de Segurança Informática que, em caso de falhas, deverá identificar ameaças e providenciar contra medidas efectivas. Assim, um nível superior de identificação dos indivíduos que interagem com o sistema, assume um carácter essencial onde as acções permitidas estão devidamente definidas. É a designada autenticação no sistema. Ou seja, para além da identificação do utilizador, a autenticação pressupõe também a definição do grau de intervenção.

3.3. CONTRIBUTO SOCIAL

O maior desafio que se coloca a qualquer sistema de gestão da informação promovido pelo governo é a sua aceitação e credibilidade pública, ou seja, que tipos de percepção têm os munícipes em relação ao mesmo. Existe, por vezes, uma grande distância entre o as escolhas do projecto – âmbito ou tecnológicas – e as expectativas ou preconceitos idealizados pelos diferentes utilizadores, levando muitas vezes à frustração destes. Por isso devem ser acauteladas estratégias de comunicação, de forma a tornar esta desigualdade mais ténue. Estas acções devem numa primeira fase estabilizar os conhecimentos dos funcionários públicos, através de acções de formação. Só numa segunda fase, e promovendo os serviços electrónicos em meios tradicionais, o alvo da comunicação deverá ser o munícipe. Nesta fase pode-se contar com a ajuda preciosa dos funcionários públicos, mas serão necessários outros meios, nomeadamente, apresentações públicas, posters, outdoors, brochuras e inevitavelmente, a Internet.

Uma outra forma de conseguir a devida aceitação e credibilidade pública é promovendo a participação dos munícipes na decisão das aplicações prioritárias da gestão da identificação do munícipe sobre o ponto de vista destes. Desta forma, será desenvolvido o sentimento de pertença e aproxima o âmbito do projecto às necessidades e expectativas dos munícipes, sendo a probabilidade de sucesso maior.

No entanto, a forma mais eficaz para alcançar um maior número de utilizadores é através da colocação na prática de procedimentos e serviços que permitam atestar as reais vantagens, bem como aquelas que percepcionadas pelos os munícipes.

3.4. DEONTOLOGIA E LEGISLAÇÃO

Aspectos éticos ligados a todas as fases do ciclo de vida da Informação de carácter privado tornaram-se uma questão central na sociedade e que não podem ser negligenciados. Os sistemas de identificação individual requerem algum tipo de registo para consulta. Nos sistemas actuais, esse registo é normalmente efectuado

em base de dados digitais que, pela sua fiabilidade, capacidade e rapidez de processamento, apresentam-se como a aposta clara dos decisores. No entanto, não devem ser descurados os riscos associados aos mesmos, sendo a ignorância em questões de segurança, por si só um risco.

O registo de dados pessoais em bases de dados levanta sérias questões sobre a privacidade do indivíduo. Há alguns cenários que ilustram os riscos associados. Imagine-se o caso do indivíduo facultar os seus dados pessoais para determinado fim. Essa informação é depois cedida a terceiros que a correlacionam com outros dados, usando a informação daí resultante para fins com os quais o indivíduo em análise nunca concordou explicitamente. Ou então, o cenário em que a entidade que gere a base de dados sofre um ataque físico, informático ou de abuso de confiança pelos seus colaboradores, e há fuga de dados em favor de pessoas que à partida não os deveriam ter. Estes riscos reais envolvem ilegalidades que violam a privacidade e propriedade intelectual dos indivíduos e, no limite, poderão ser classificados como roubo da identidade.

Existem outras contendas legais que envolvem questões de direito de autor e de propriedade intelectual, bem como a privacidade, espionagem comercial, e dados pessoais, havendo a necessidade de associar a estes aspectos noções de imputabilidade, porventura difíceis de identificar. Neste caso, deve ser a Gestão da Informação – partindo da descrição de papéis – a fazer a ligação entre os aspectos legais e a organização, devendo agir pró activamente, de forma a evitar que a lei seja infringida.

Os governos existem para servir o cidadão e não para se servir dele. A variedade de documentação que qualquer cidadão deve possuir para se identificar perante a miríade de entidades da Administração Pública – porque não é só um problema local, se bem que existem esforços por parte do actual governo de forma a responder precisamente a este problema – bem como os procedimentos necessários à obtenção desses documentos, ou para obter outros – certidões, registos, atestados – obrigam a enorme dispêndio de tempo, dinheiro e energias. Em tudo contrários ao fixado no artigo 267.º da Constituição da República Portuguesa que determina que *"A Administração Pública será estruturada de modo*

a evitar a burocratização, a aproximar os serviços das populações..." ou o que estabelece o Código do Procedimento Administrativo, no seu artigo 10.º: *"A Administração Pública deve ser estruturada de modo a aproximar os serviços das populações e de forma não burocratizada, a fim de assegurar a celeridade, a economia e a eficiência das suas decisões"*. A identificação integrada do munícipe contribui para o agilizar dos procedimentos da administração pública.

Na organização dos dados do sistema, devem obrigatoriamente ser tidas em conta as determinações constitucionais e legais previstas para o tratamento informático de dados pessoais. É constitucionalmente proibida a *"atribuição de um número nacional único aos cidadãos"* (n.º 5 do artigo 35.º da Constituição da República Portuguesa). Contudo, o contexto local do modelo não se sobrepõe a esta lei. No entanto, é obrigatória a referência à limitação existente quanto à interconexão de dados pessoais – ainda que contornável tecnologicamente – (artigo 9.º da Lei n.º 67/98 – Lei da Protecção de Dados Pessoais), razão pela qual o processo de implementação do sistema deverá ser avaliado pela Comissão Nacional de Protecção de Dados[13].

Por fim, a actual legislação deve ser ponderada a fim de promover ganhos substanciais de produtividade que as soluções tecnologias tendem a oferecer às organizações. Por exemplo, a delegação de autorização a terceiros, é algo tecnologicamente simples de resolver. No entanto poderão se verificar constrangimentos legais.

3.5. ECONÓMICOS

Uma das primeiras considerações feitas neste trabalho é que a informação é um recurso organizacional valioso. No entanto, e devido ao cariz do seu conteúdo, estes recursos não são transaccionáveis. É necessário encontrar outras formas de financiamento.

[13] http://www.cnpd.pt/

O esforço financeiro associado a este tipo de projectos é suportado, em grande parte, pelo orçamento da administração local, que deriva directamente do orçamento de estado. Contudo, e fazendo valer a parceria privada, no enquadramento da empresa municipal, estes deverão contribuir com diversos recursos, nomeadamente humanos, tecnológicos e financeiros.

O 6º Programa Quadro comunitário tem desenvolvido diversas iniciativas, nomeadamente o plano de acção e-Europe 2005, no sentido de ajudar os governos locais. Os Fundos Estruturais desempenham aqui um papel fundamental. Recorde-se que as verbas estimadas destes fundos para o período compreendido entre 2000 e 2006 são cerca de 10 biliões de euros, só no contexto da sociedade da informação[14].

O plano e-Europe 2005 pretende criar redes alargadas que, mais do que municípios, liguem países. Os municípios mais isolados, em áreas rurais, poderão condicionar todo o esforço desenvolvido pela sociedade da informação ao não conseguir acompanhar o ritmo dos mais desenvolvidos. Cabe a estes últimos, ajudar de forma incondicional para que, todos sigam ao mesmo ritmo. A ajuda proporcionada pelos fundos estruturais, assim como a partilha do conhecimento, permite alcançar uma maior coesão entre todos os municípios da União Europeia.

3.6. MODELOS DE GESTÃO DO SERVIÇO

A entidade responsável pela gestão do sistema de identificação municipal deve ser alvo de profunda reflexão. Existe um conjunto de critérios que devem ser levados em consideração e que poderão variar conforme a especificidade de cada município não sendo taxativa a aplicação de um ou outro modelo. Contudo, e antes de mais, deve ser definido que tipo de serviço é a gestão da identificação do munícipe. Recorrendo à metodologia proposta por J. Amado da Silva (2004), podem ser encontradas duas propriedades que ajudam a distinguir os diferentes serviços. Apesar de uma visão simplista, reconhecida aliás pelo próprio autor, encaixa-se

[14] http://europa.eu.int/comm/regional_policy/sources/docgener/evaluation/doc/information_society.pdf

perfeitamente para o efeito. As propriedades são a rivalidade e a exclusão do serviço. A ausência ou presença de qualquer uma coloca o serviço em diferentes estádios. Um serviço apresenta rivalidade quando o seu uso impede ou diminui a utilização por outra pessoa. Por exemplo o uso de telefone. Por seu lado, a exclusão é uma característica que impede o acesso a terceiros, mesmo que este esteja disponível, como é o caso do acesso a uma área reservada. Um serviço público é aquele que é simultaneamente não rival e não exclusivo, sendo um serviço privado, aquele que é rival e exclusivo.

A figura seguinte identifica as combinações possíveis do cruzamento entre a exclusão e a rivalidade na gestão do serviço.

		exclusão	
		sim	não
rivalidade	sim	PRIVADO	COMUM
	não	MONOPÓLIO NATURAL	PÚBLICO

Figura 3-2 Natureza dos serviços[15]

Dadas as particularidades do serviço de identificação do munícipe, isto é, os indivíduos podem-se identificar sem rivalizar com terceiros e, ao mesmo tempo, estar automaticamente incluído no sistema de gestão da identificação. Pode-se, por conseguinte, afirmar que a gestão da identificação do munícipe é um serviço público.

Ao se analisar os objectivos últimos dos sectores públicos e privados, pode-se perceber a razão da sua diferenciação. O sector privado visa a optimização dos lucros baseado nas elementares leis da oferta e da procura. Por seu lado, o sector

[15] Proposto por J. Amado da Silva (2004, p.27)

público propõe-se a providenciar o bem-estar das populações, satisfazendo as lacunas do mercado, ou seja, dando resposta em áreas onde não há mercado concorrencial.

Após esta breve caracterização dos serviços, importa então explorar os cenários prováveis em que a gestão do sistema de identificação do cidadão potencialmente melhor se encaixa.

Analise-se então os casos clássicos de gestão: o Serviço Público, providenciado pela própria autarquia; a Empresa Municipal; e por fim, a concessão do serviço ao sector privado ou privatização. Existem características em cada um dos modelos que permitem facilitar a adopção de uns em detrimento dos outros. Não parece que o total controlo por parte do sector privado seja a melhor aposta, devido à elevada importância transversal do uso da identificação nos diversos quadrantes municipais. Por seu lado, o serviço municipalizado sofre do preconceito relacionado com a sua gestão. J. Amado da Silva (2004, p.41) aponta como principal factor, a dificuldade de identificar indicadores mensuráveis do desempenho dos gestores públicos. A este problema de liderança dos serviços públicos, acresce a difícil harmonização com o sector privado. De forma a ser conseguido o máximo potencial da gestão integrada público/privada da identificação dos munícipes, a empresa pública, assente em fortes parcerias privadas, parece ser o melhor enquadramento para a gestão do serviço de identificação do cidadão. Este tipo de empresa frui de controlos mais apertados na eficiência e qualidade dos serviços prestado, por iniciativa privada, voltando a estratégia da mesma para a satisfação dos munícipes.

3.7. SUMÁRIO

O presente capítulo visou explorar as condições essenciais para a implementação de um sistema de identificação de munícipes.

Diariamente, é solicitada a identificação por parte da Câmara Municipal, do hospital, do Centro de Saúde, entre muitas outras instituições com as quais se interage. Ora, numa sociedade moderna, onde o tempo é considerado precioso, torna-se fundamental simplificar todo este processo, tantas vezes burocrático,

cansativo e moroso, sem nunca esquecer a manutenção da segurança e privacidade dos utilizadores.

Actualmente, existem iniciativas nacionais e projectos comunitários de apoio, com vista à investigação e ao desenvolvimento no âmbito da temática da sociedade de informação. Contudo, subsistem alguns factores a ter em consideração por parte das organizações que desenvolvem este tipo de projectos: objectivos; tipo de hardware e software; procedimentos efectuar e tipo de pessoas intervenientes no processo.

Estes sistemas de informação operam em diferentes níveis de organizacionais (operacional, conhecimento, gestão, estratégico), conforme o grau de complexidade exigido. O sucesso da comunicação entre os diversos níveis depende de uma eficaz gestão de identificação do indivíduo. Para tal, é necessário apostar numa integração entre os níveis e as entidades participantes.

Para reconhecer e interpretar os instrumentos de identificação, poder-se-á utilizar as tecnologias já existentes no mercado e adaptá-las à nossa realidade, como é o caso da linguagem Java ou os sistemas de gestão da base de dados Oracle. Assim, a redução de custos e de tempo será significativa.

Para que o processo de adopção do modelo de identificação seja eficiente, é crucial que ambos políticos e administradores estejam em sintonia, tendo em conta as características próprias das comunidades, não negligenciando aquelas pessoas com mais dificuldades em perceber e utilizar a tecnologia.

Ora, o governo electrónico terá sucesso se este for assimilado pelos munícipes. Para tal, torna-se necessário se efectuar um trabalho de campo, ou seja, investir na formação quer da Administração Pública, quer dos utilizadores, para que todos se adoptem à nova realidade. Por outro lado, tem que existir uma grande componente comunitária entre os mentores do sistema e os utilizadores, com o intuito de diminuir a discrepância entre a teoria e a prática, bem como corresponder às expectativas dos destinatários.

Sem dúvida que o meio mais eficaz de se chegar à massas e de alcançar a aceitação pública, é através da comunicação, da divulgação e, sobretudo, da publicitação.

Esta nova política de gestão da informação que se propõe deve ter em atenção 4 aspectos fundamentais: confiança, integridade, legislação existente, disponibilidade. Só assim será possível desenvolver um sistema prático e autêntico, onde o utilizador se sinta seguro, confortável e autónomo.

4 PROPOSTA E DISCUSSÃO DE UM MODELO

O principal objectivo deste trabalho não é apresentar o estado da arte em relação às tecnologias disponíveis no mercado referentes aos sistemas de identificação individual. Mais do que isso, pretende-se apresentar um modelo conceptual que guie uma reforma nas práticas das pessoas – incluindo aquisição de novas competências –, bem como a inovação dos procedimentos actuais, tendo em vista o serviço público e a satisfação dos munícipes. Nesta linha de pensamento, Luís Gouveia (2004, p.14) afirma que "*o sistema de informação é bem mais do que a utilização de instrumentos tecnológicos, tais como o computador e os SGBD, logo, para cumprir as suas funções é necessário assegurar, inclusive, a organização dos recursos humanos disponíveis e explicitar e estabilizar os processos utilizados para assegurar o funcionamento da organização*".

Nas sociedades modernas, a informação é tida como um recurso valioso, daí decorre a denominação Sociedade da Informação. Por tal, é imperativo existirem

infra-estruturas adequadas para a recolha, armazenamento, processamento, representação e distribuição da informação, de forma a esta poder ser utilizada na tomada de decisões (Luís Gouveia, 2004).

A informação, na sua acepção enquanto recurso, necessita de uma visão estratégica em relação à sua gestão. Esta visão será o garante da **integração** e da **inter operacionalidade** entre os diferentes departamentos municipais e as empresas. A integração, pela simplificação no uso e partilha da informação. Já a inter operacionalidade, assegura que a troca de informação se realiza observando padrões semânticos, suporte tecnológico e permissões.

A gestão da identificação é considerada pela Comissão Europeia como um dos pilares no relacionamento entre os cidadãos e a administração pública. Na ordem do dia estão temas como o eEuropa 2005, o i2010, a Agenda de Lisboa, o alargamento da União Europeia, a cidadania, a segurança e a estabilidade. Estes prestam enormes contributos no sentido da modernização da administração pública.

Esta modernização obriga a uma mudança de paradigma. A administração pública, através da facilitação dos governos electrónicos, deverá promover a inclusão dos desfavorecidos, de forma a proporcionar condições que permitam a participação na vida activa das sociedades, tendo como base uma gestão eficaz e eficiente, contribuindo, desta forma, para o aumento da produtividade.

A Figura 4-1 permite enquadrar a Gestão da Identificação no contexto da Administração Pública.

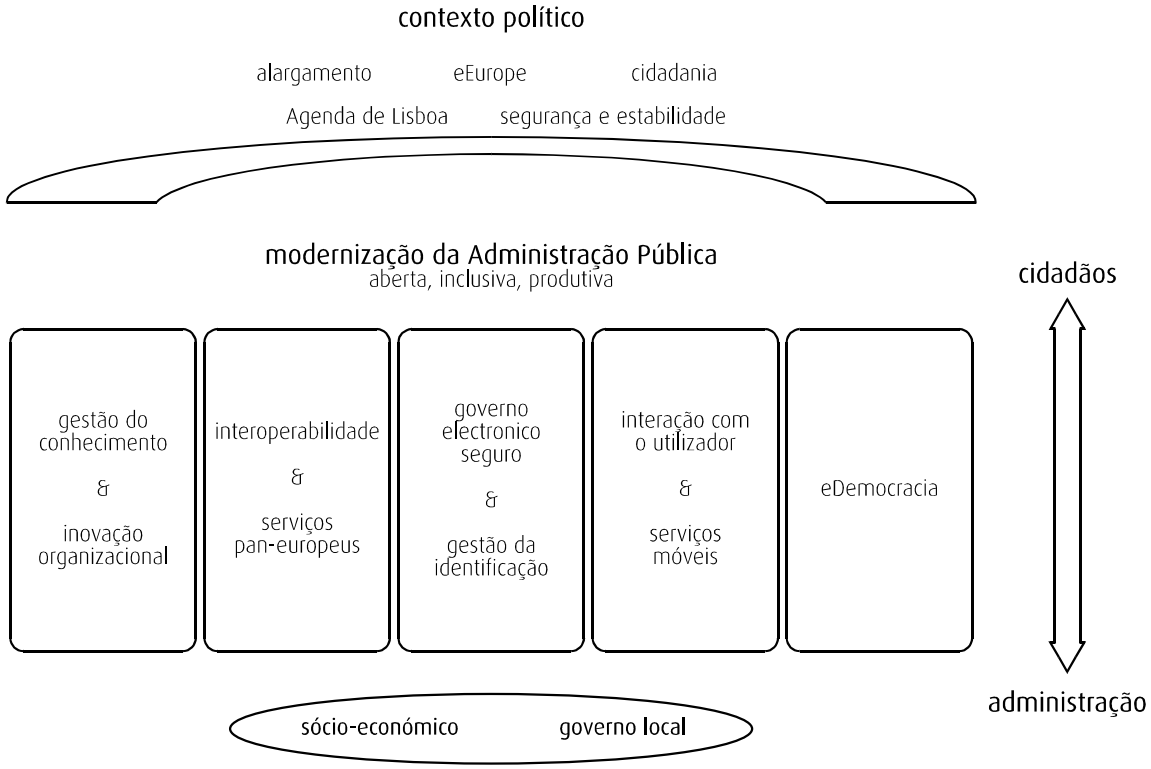

Figura 4-1 Papel da Gestão da Identificação na Administração Pública[16]

A materialização em cidades digitais, geradas a partir dos *local e-government*, disponibilizam um conjunto de serviços em linha. Neste enquadramento, a gestão da identificação potencia a aproximação do relacionamento na oferta de serviços públicos, orientações gerais, gerando oportunidades de e-lerning, e-commerce, e-business e actuando, deste modo, nas esferas culturais, sociais e económicas.

[16] Adaptado da visão da Comissão Europeia, no portal para a Sociedade da Informação: http://europa.eu.int/information_society/activities/egovernment_research/focus/index_en.htm

4.1. ENQUADRAMENTO CULTURAL E SOCIO-ECONÓMICO

Todas as iniciativas requerem empenho para que possam traduzir-se em proveitos. Partindo deste princípio básico, também a gestão da identificação dos munícipes requer a concertação de esforços em virtude de serem alcançados benefícios.

Luís Gouveia, no exercício das funções de orientação, defende que a gestão da identificação individual, baseada num sistema de cartões, deve observar duas condicionantes:

- Ou está associada ao território ou ao poder político;
- Ou envolve interesses económicos partilhados por diferentes empresas.

Ora, no caso dos municípios, e pelo seu forte relacionamento com o território, a satisfação destas condicionantes apenas se torna viável quando promovidas pelo poder local, ou em sintonia com este, devendo chamar a si a liderança na tomada de decisões e na dinamização do projecto.

Uma iniciativa associada com meios de identificação tem impacto – quer ao nível dos esforços, quer ao nível dos benefícios, ainda que em diferentes graus – nos distintos vectores da sociedade, ou seja, ao nível: económico; social; cultural. Esta implica algum grau de mudança de paradigma que vai além dos sistemas de informação, obrigando o repensar da essência da própria organização, as rotinas, funções e qualificações (André Alves e José Moreira, 2004 p. 38), dando lugar a eventuais mudanças organizacionais. Estas envolvem um risco considerável, mas também uma maior expectativa em relação aos seus benefícios.

Estas mudanças trazem associadas investimentos financeiros intensivos, pelo que, como principal promotor, o município deverá desenvolver um maior esforço no sentido de financiar o desenvolvimento, a implementação e a sobrevivência do projecto. Contudo, é espectável que as organizações privadas envolvidas participem também a este nível. Estes esforços têm um impacto a curto prazo ou até mesmo

imediato, traduzindo-se como benefícios directos, advindos de um serviço agilizado e de uma gestão mais eficaz dos recursos existentes.

Este clima de mudança implica, a médio prazo, um impacto sobre o Balanço Social das organizações. Novas oportunidades e necessidades serão geradas, enquanto outras tendem a perder expressão. Importa então projectar a mudança também nas pessoas. Estas deverão perceber que irão actuar num clima mais volátil, onde serão premiados aqueles que mais facilmente se adaptem a novas realidades, gozando por isso de um reportório ao nível do conhecimento mais vasto. Uma nova janela de investigação surge aqui, envolvendo a requalificação dos recursos humanos das organizações, nomeadamente nos serviços públicos, através da formação, seja ela baseada nos métodos tradicionais, ou baseada no *e-learning*, uma vez que as tecnologias não substituem o Homem, apenas servem como suporte à sua actividade. Contudo, os recursos humanos deverão adquirir novas competências, não só relacionadas com as TIC, mas também ao nível do relacionamento, do trabalho em equipa e porque não, ao nível do empreendorismo e da inovação. É obvio que a capacidade de extrair valor acrescentado é menor do que o potencial elevando-se, assim, a necessidade de atingir níveis superiores de desempenho.

Numa perspectiva a longo prazo, a identidade territorial é geradora de coesão social. Veja-se o caso da bandeira nacional, o símbolo de uma nação, dum povo, dum território e que no ano de 2004, aquando do campeonato europeu de futebol, gerou uma forte aderência à manifestação do patriotismo como poucas vezes visto. São externalidades, ou benefícios indirectos, associados à identificação e identidade que – aproveitando a plataforma de gestão de relacionamentos – poderão ser exploradas pelos *marketeers* no desenvolvimento de estratégias de comunicação com um maior conhecimento do seu público.

A Figura 4-2 visualiza o enquadramento do modelo atendendo aos vectores da sociedade, considerando os esforços e benefícios.

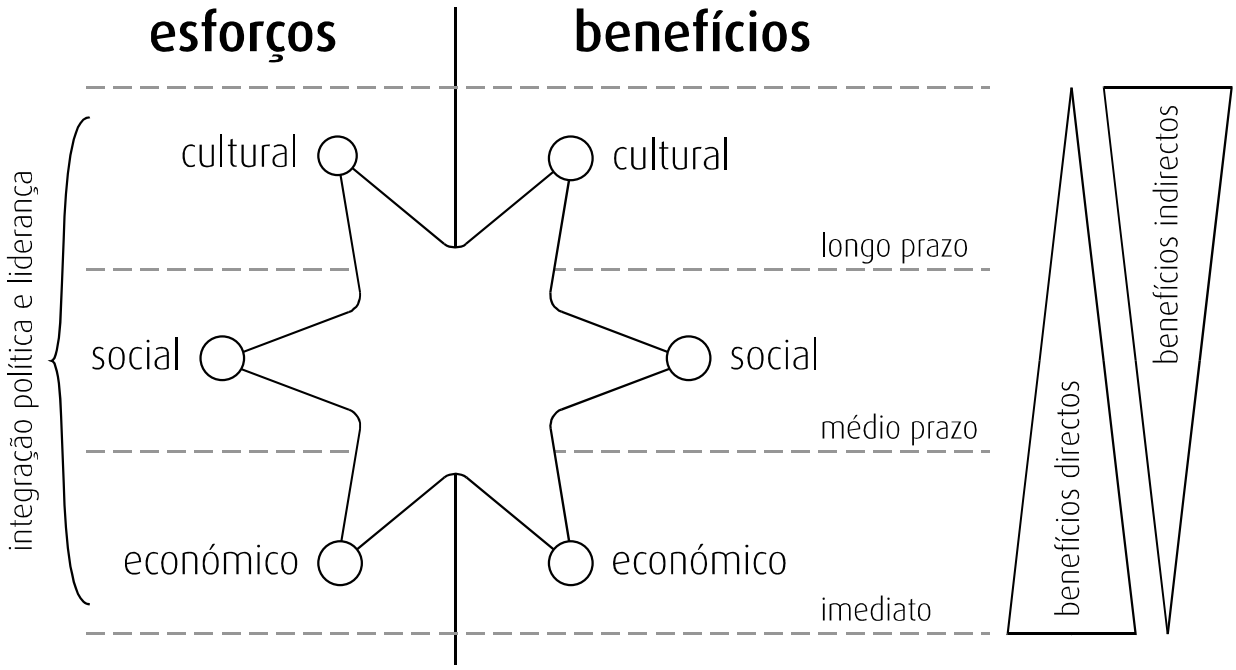

Figura 4-2 Perspectiva macro social[17]

4.2. SEGURANÇA

A segurança deverá ser uma das principais preocupações da equipa de desenvolvimento. Quando falamos de segurança ao nível do estado, independente da instância, são quase impensáveis os efeitos nefastos relacionados com falhas de segurança dada a sensibilidade da informação oficial.

Os sistemas de identificação são assentes em bases de dados transaccionais, sendo acedidas e alteradas com frequência. É então imprescindível garantir elevados padrões de segurança, nomeadamente na qualidade de autenticação dos utilizadores e na atribuição dos perfis de utilização, a fim de que estes acedam apenas às informações que lhes são relevantes. Para além de garantidas a

[17]Proposto por Luís Gouveia

confidencialidade e a integridade das bases de dados, deve-se restringir o cruzamento de dados provenientes de bases de dados públicas e privadas.

Os crimes cometidos no âmbito do digital devem ser julgados recorrendo ao enquadramento legal dos contextos tradicionais. As autoridades policiais e judiciais deverão ser capazes de lidar com estas novas ameaças de forma eficiente.

4.2.1. Infra-estrutura de segurança PKI

A criptografia tem vindo a ser desenvolvida de forma a satisfazer as necessidades correntes, nomeadamente no uso da Internet. As infra-estruturas de chaves públicas, ou PKI do inglês *Public Key Infrastructure*, envolvem métodos seguros que fornecem soluções, com maiores garantias em termos de privacidade, na autenticação e assinaturas digitais em meios digitais.

A base fundamental da PKI é a criptografia com um par de chaves assimétricas. Cada entidade tem associada um par de chaves. O par é composto por uma **chave privada**, usada na encriptação de qualquer tipo de informação digital, de tal forma que apenas uma **chave pública** possa desencriptar. A chave privada é mantida em segredo enquanto que a chave pública deverá ser partilhada com todos aqueles que necessitem de desencriptar as informações protegidas.

Sendo este par de chaves – privada e pública – assimétrico e único na sua correspondência, pressupõe-se que a informação desencriptada por determinada chave pública é fidedigna em relação à origem aquando da encriptação. Ou seja, da combinação entre chave privada e chave pública resulta a **assinatura digital**.

A Figura 4-3 sistematiza o funcionamento básico da PKI.

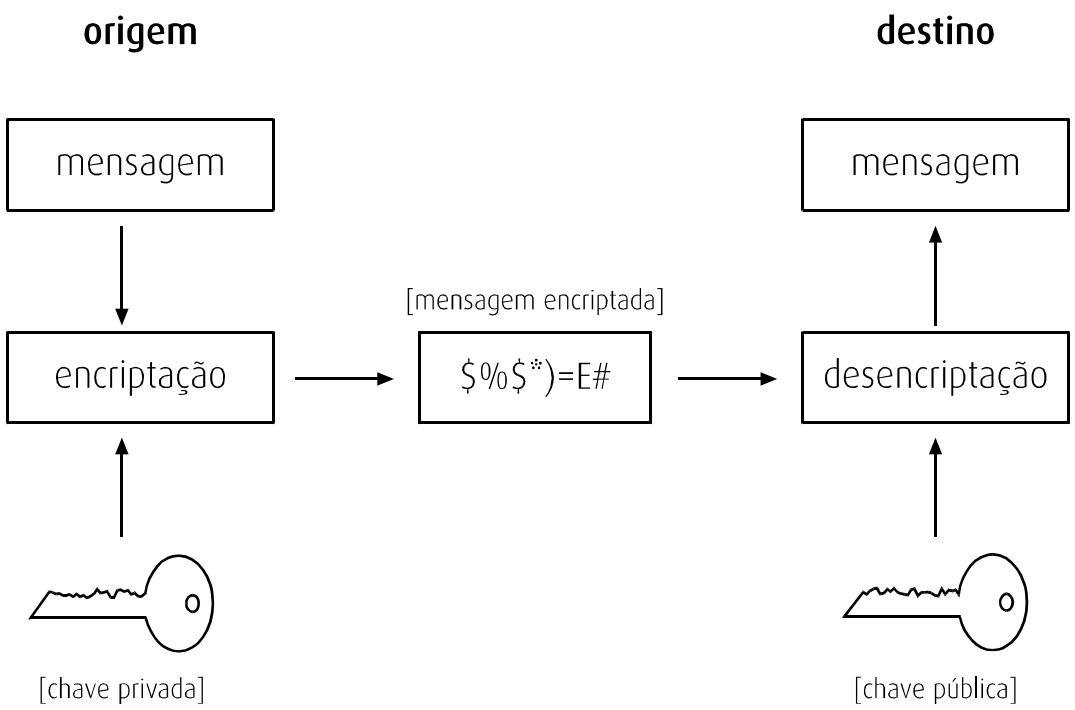

Figura 4-3 Modelo base da infra-estrutura de chave pública

A aplicação de PKI permite satisfazer necessidades de segurança ao nível das:

- **Aplicações**, pela garantia da autenticidade e integridade manifestadas na segurança da troca de mensagens entre os diferentes sistemas envolvidos;
- **Infra-estruturas**, pela certificação conferida aos sistemas envolvidos;
- **Utilizadores**, na autenticação da sua assinatura digital.

De forma a se garantir a confiança de uma chave pública, deve-se recorrer a certificados. Existem vários certificados implementados no mercado, todavia o X.509 v3 tem-se destacado dos demais.

È importante a existência de autoridades de confiança que atestem a autenticidade destes certificados. O projecto Pegasus[18] – vulgarmente designado cartão do cidadão –, promovido pelo governo português, pressupõe a existência de uma Entidade Certificadora Electrónica do Estado (ECEE). Esta será a instância máxima e mais fidedigna, na atribuição de certificados. Será também responsável pela acreditação de outras entidades certificadoras (EC) hierarquicamente inferiores, como poderão ter os municípios uma dependência.

É obrigatório garantir a privacidade da chave privada. As assinaturas digitais garantem a participação do sujeito em determinada transacção, dificultando o repúdio da mesma. Se este conseguir provar que a suas chaves privadas estão comprometidas e potencialmente a ser usadas por terceiros, então toda a infra-estrutura estará em risco.

4.3. CENÁRIOS PRÁTICOS DO IDENTIFICADOR

Os sistemas de identificação requerem um identificador *(token)*, algo que pertença ao indivíduo e que possa ser utilizado na sua identificação perante terceiros. Os cartões *smart cards* e a biometria afiguram-se como os *token* privilegiados para essa função. Analise-se então as suas características.

4.3.1. Tokens

CARTÕES SMART CARDS

Os *smart cards* são cartões de plástico, semelhantes aos cartões de banda magnética. Porém, incorporam microprocessadores e unidades de memória como componentes. Derivados da evolução que têm sofrido os cartões ao longo dos anos, os *smart cards* diferenciam-se em relação aos seus precedentes pela sua segurança. Estes gozam de módulos de segurança dos dados inscritos no seu *chip*, permitindo ainda proteger dados noutros sistemas. As ISO 7816 e ISO 7810 normalizam o

[18] Disponível para mais informações o relatório final da prova de conceito no sítio do cartão do cidadão em http://www.cartaodocidadao.pt/images/stories/relatorio_prova_conceito.zip

formato do corpo, a posição e a forma dos contactos do chip, as características eléctricas, os protocolos de comunicação, a robustez e a funcionalidade do cartão.

A memória dos *smart cards*, protegida por PIN, permite armazenar os dados identificativos do sujeito, assim como o número único de munícipe e o número de cliente das entidades parceiras, bem como os certificados e as chaves privadas de segurança, usados nas PKI.

Para além da segurança lógica dos *smart cards*, estes possuem potencial para incorporarem medidas de segurança física, através de um conjunto de mecanismos de personalização da aparência do mesmo, de forma a evitar a clonagem dos cartões, dos quais se destacam:

- **Padrões de alta resolução e elevada complexidade,** impossibilitando a reprodução com os meios tradicionais;
- **Tinta de variação óptica,** tendo um comportamento diferenciado conforme o ângulo de visão;
- **Tinta invisível,** que permite imprimir informação que apenas é visível com radiações de luz especial;
- **Hologramas**;
- **Personalização** do cartão com os dados pessoais do indivíduo e a sua fotografia.

A emissão do cartão do munícipe envolve um conjunto alargado de entidades e diferentes relacionamentos entre elas conforme demonstrado na Figura 4-4.

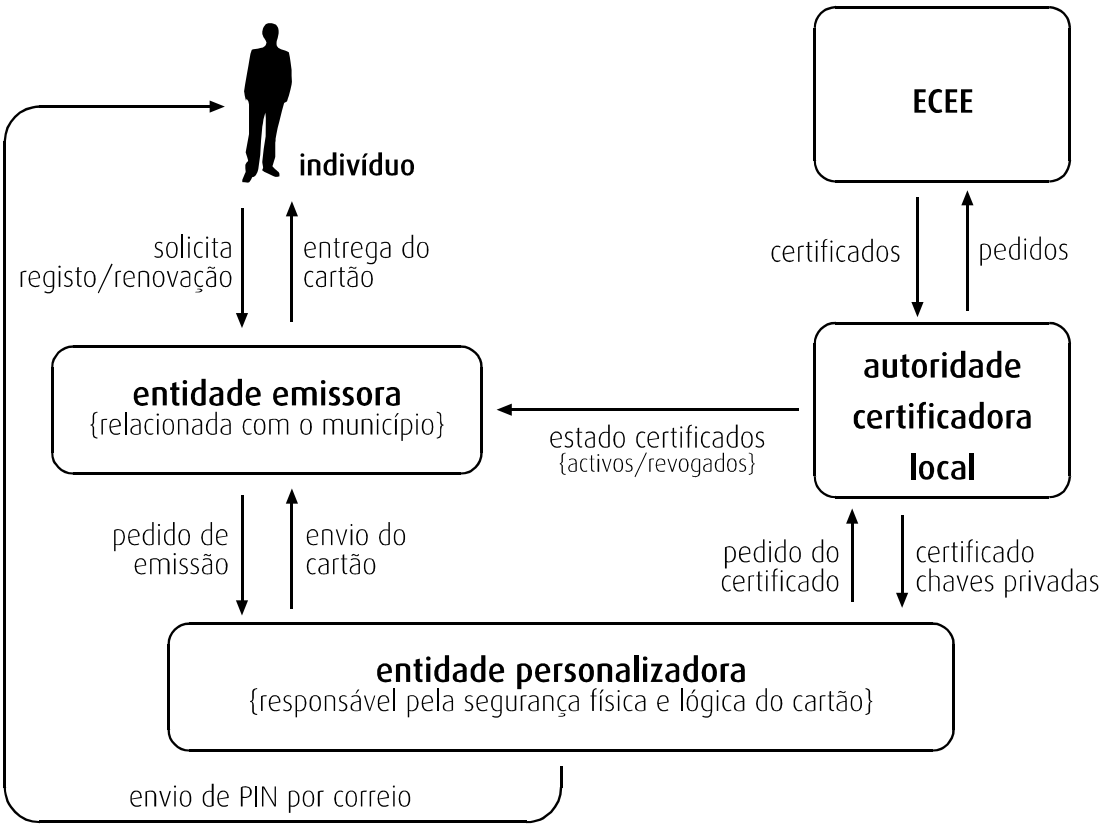

Figura 4-4 Ciclo de vida do cartão

BIOMETRIA

Os seres humanos são portadores de características que os tornam únicos. A análise destas características permite identificar os indivíduos. Estas enquadram-se em dois níveis diferentes de análise:

- **Físicas**, que envolve a identificação pelas veias das mãos, impressão digital, geometria facial, geometria da mão ou a íris;
- **Comportamentais**, que identifica através da análise da voz, de assinatura ou da caligrafia.

As tecnologias biometricas comportamentais proporcionam um baixo nível de fiabilidade, ou seja, o seu carácter comportamental está sujeito à manipulação

propositada e à distorção por factores externos, como é o caso do ruído de fundo da análise da voz. Logo, não é aconselhável a sua aplicação na gestão da identificação. Contudo, as soluções propostas pela análise de características biometricas físicas oferecem um conjunto de opções que satisfazem as necessidades para a gestão da identificação. A Figura 4-5 compreende um quadro comparativo entre diferentes tecnologias pelo seu desempenho em algumas características chave.

	Maturidade	Fiabilidade	Velocidade	Estabilidade	Custo
Veias das mãos	Baixa	Muito alta	Alta	Muito Alta	Alto
Impressão digital	Alta	Média	Alta	Média	Médio
Geometria facial	Media	Média	Alta	Média	Médio
Geometria mão	Alta	Alta	Alta	Média	Médio
Íris	Alta	Muito alta	Média	Alta	Alto

Figura 4-5 Comparação das tecnologias biometricas físicas

Um sistema biometrico engloba geralmente as seguintes componentes:

- **Captura**: que consiste na aquisição da amostra biometrica;
- **Extracção**: que converte a amostra para um formato intermédio;
- **Padrão**: transformação do formato intermédio em formato padrão para ser arquivado;
- **Comparação**: comparação de uma amostra com o padrão arquivado.

Ao processo de transformação de informação analógica – como é o caso de uma impressão digital – em informação digital dá-se o nome de digitalização. Neste processo há sempre perda de informação em relação ao original. Esta característica é provavelmente a maior ameaça ao sistema, pois presume-se que este seja capaz

de rejeitar impostores e de aceitar o utilizador válido. Existe um método para aferir a performance dos sistemas, levando em consideração duas variáveis, a **taxa de falsa rejeição (FRR)**, do inglês *False Reject Rate*, e **taxa de falsa aceitação (FAR)**, do inglês *False Acceped Rate*. A Figura 4-6 demonstra a correlação entre as variáveis, podendo-se verificar que um sistema poderá ser afinado para ser permissivo, tendo uma alta FRR, logo uma baixa FAR, ou então, um sistema restritivos, onde a FRR é baixa, mas a FAR é alta.

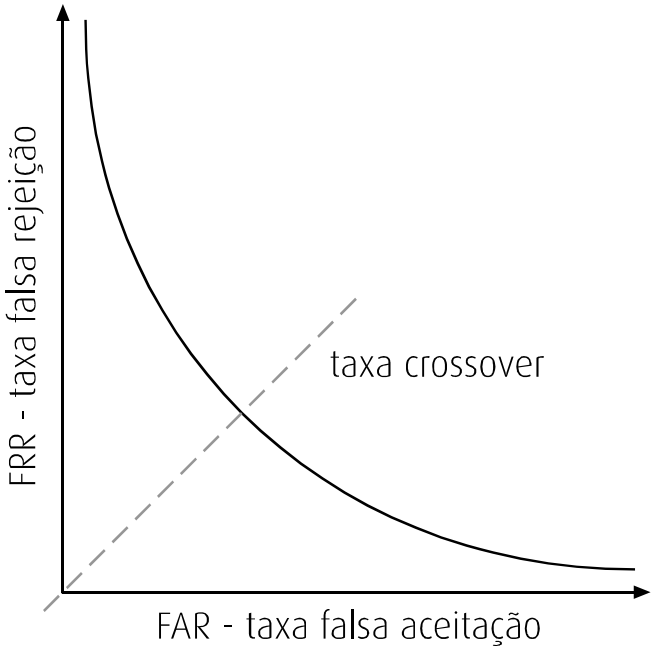

Figura 4-6 Correlação falsa rejeição e falsa aceitação

A figura permite ainda vislumbrar um ponto crítico onde a FAR iguala a FRR, sendo designado como taxa *crossover*. Segundo Mike Hendry (1997, p.70) as taxas *crossover* actuais andam abaixo dos 0,2% e algumas mesmo abaixo dos 0,1%.

É espectável que as taxas tendam a comportar-se de forma inversamente proporcional à sua utilização. O sistema afina automaticamente o padrão arquivado de acordo com a última utilização. Daqui decorrem duas perspectivas. Por um lado, um indivíduo que utilize esta tecnologia com frequência será facilmente identificado. Por outro lado, um indivíduo que utilize esta tecnologia apenas pontualmente é propenso a ter problemas. O corpo humano sofre alterações ao longo do tempo – pode ganhar ou perder volume, por exemplo – pelo que numa

situação limite o sistema poderá mesmo não reconhecer o indivíduo. Neste caso, será obrigado a efectuar um novo processo de registo *(enrollment)*.

O índice de segurança associado a esta tecnologia poderá ainda ser ampliado com o uso combinado da característica biometrica e um código PIN que apenas o utilizador conheça.

4.3.2. Modelos de aplicação prática

O mercado oferece inúmeros cenários para a gestão da identificação. São destacadas as três propostas que apresentam um maior potencial para a aplicação prática, pelo recurso a rotinas amplamente aceites. Todas elas observam critérios de privacidade e de segurança rigorosos e algumas atingem um elevado grau de maturidade.

A primeira proposta é baseada em *smart-cards*, enquanto que a segunda em características biometricas do sujeito. Já a terceira proposta resulta da combinação das duas anteriores.

Todos os cenários apresentados encerram vantagens e desvantagens que passarão a ser exploradas.

SMART-CARD COM SUPORTE PKI

A utilização dos cartões *smart cards* na identificação individual tem sido amplamente adoptada, sendo já um caso clássico na identificação. A principal diferença entre os *smart cards* e os outros cartões reside na existência de um chip. Este não é mais do que um microcomputador que contém determinada memória ROM usada para o sistema operativo, memória RAM, uma central de processamento e a EEPROM, onde estão alojadas as aplicações.

A identificação é baseada em algo que sabemos – o PIN – e algo que temos – o *smart card*.

Uma das principais virtudes dos *smart cards* é poder desempenhar as suas funções fora de linha, em contextos onde não é necessário recorrer a informações

actualizadas em tempo real – como é o caso da aplicação de uma assinatura digital – permitindo uma interacção mais rápida e sem custos de comunicação.

De uma forma resumida, a Figura 4-7 apresenta as valências de autenticação e de assinatura digital proporcionadas pelos *smart cards*, recorrendo a PKI.

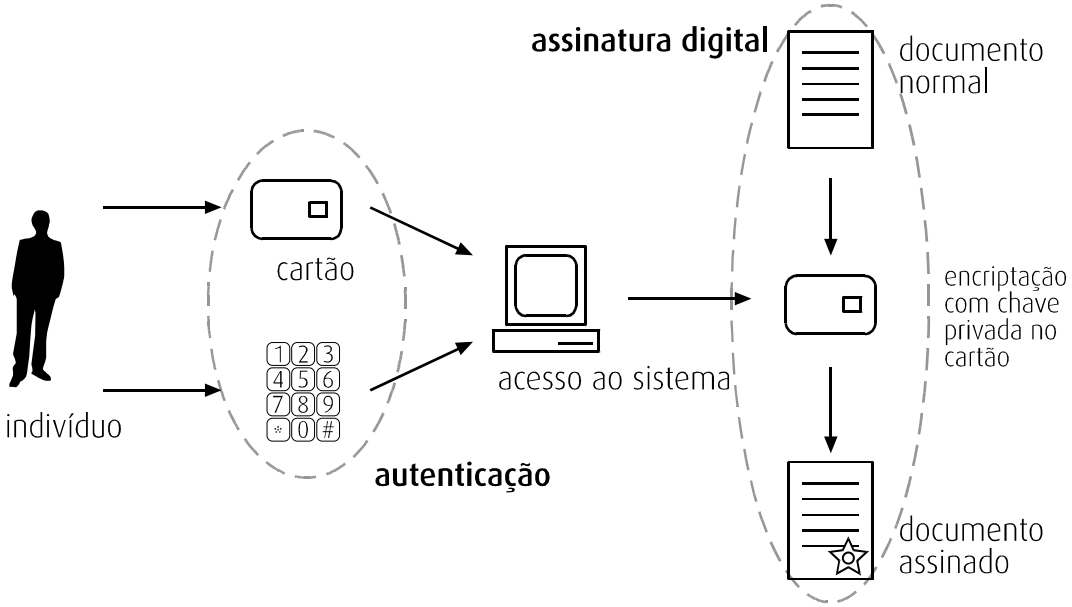

Figura 4-7 Arquitectura de autenticação e assinatura, usando *smart cards* e PKI

Este tipo de identificação permite ainda a partilha do suporte por diferentes entidades. Ou seja, um único cartão poderá responder às necessidades de diversas organizações ao ser possível instalar diferentes aplicações na sua memória. O acesso a estas aplicações obedece a políticas de segurança previamente definidas de tal forma que as organizações possam decidir partilhar toda ou apenas parte da informação, ou ainda ter somente acesso exclusivo à aplicação.

A abstracção teórica apresentada na Figura 4-8 permite perceber o potencial inerente à funcionalidade multi aplicacional.

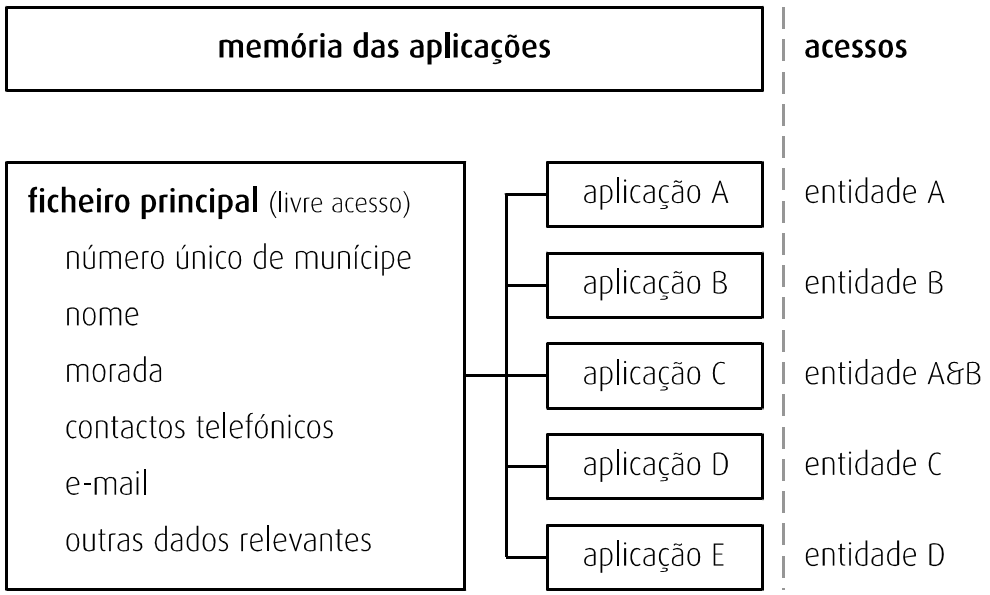

Figura 4-8 Estrutura multi aplicacional dos *smart cards*

Como principais vantagens podem-se destacar as seguintes:

- **Processo maduro**, implementado com sucesso em diferentes contextos;
- O utilizador é portador das suas chaves privadas;
- Segurança física e lógica;
- Possibilidade de autenticação **mesmo na ausência de comunicação** com sistema central;
- **Capacidade multi aplicacional,** que permite a identificação perante múltiplas entidades.

As principais considerações negativas a esta abordagem à identificação são as seguintes:

- O esquecimento do código PIN;
- A possibilidade de empréstimo do cartão a terceiros;

- A perda ou roubo do cartão;
- Possibilidade de se danificar fisicamente.

BIOMETRIA E PKI

A biometria fornece às PKI novos potenciais no que se refere à autenticidade da identificação dos indivíduos. Pelas suas características intrínsecas – a biometria é algo que somos –, a identificação não requer a memorização dum PIN e não existe um *token* que possa ser partilhado ou perdido, reduzindo a capacidade de repúdio. A empresa Daon (2003) aponta três aspectos importantes resultantes da combinação de tecnologias biometricas com PKI, são eles:

- **Facilidade de uso e segurança** da biometria na autenticação de indivíduos;
- **Custo reduzido** de propriedade centralizada da PKI;
- **Ubiquidade** e conveniência do conceito centralizador.

Após a captura da amostra biometrica por um terminal de interface, a mesma é enviada a um servidor de autenticação para processamento. Existe uma comparação com os dados existentes na base de dados biometrica, a fim de se identificar o indivíduo. Com a informação da identidade recolhida a partir da base de dados, dá-se a autenticação num cofre baseado em módulos de segurança por hardware – ou HSM do inglês *Hardware Security Modules* – onde estão armazenadas as chaves privadas do indivíduo. É nestes dispositivos que ocorre a assinatura digital, para que as chaves privadas nunca estejam expostas.

A Figura 4-9 ilustra a arquitectura de um sistema de assinaturas digitais sustentada em PKI e biometria.

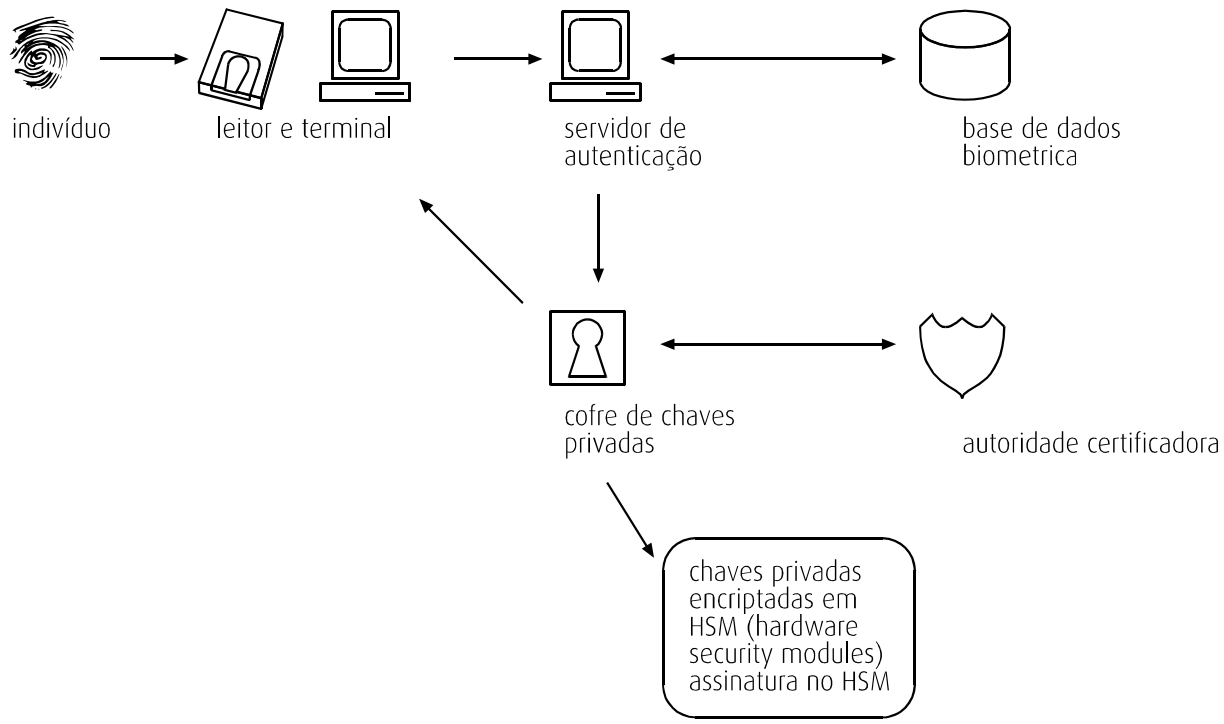

Figura 4-9 Arquitectura de identificação por biometria com uso PKI[19]

Os promotores deste modelo sintetizam da seguinte forma um conjunto de vantagens a este associadas:

- A autenticação por biometria **reduz o nível de repúdio** e o risco de roubo ou espionagem;
- **Redução de custos** de propriedade associados à infra-estrutura centralizada;
- **Escalabilidade do sistema** ao permitir responder a necessidades de grupos largamente populosos, proporcionando um desempenho assinalável ao responder num curto espaço temporal;
- Possibilidade de **auditar profunda e rapidamente** os eventos ocorridos no servidor;

[19] Proposta apresentada pela Daon (2003)

- A política de autenticação assegura a consistência na aplicação de níveis de segurança.

No entanto, este modelo apresenta algumas insuficiências que convém ter presente no momento da tomada de decisão. São elas:

- No processo de registo poderá ocorrer o roubo de identidade ao associar uma amostra biometrica de terceiros;
- É questionável a tutela externa das chaves privadas;
- Dependência da comunicação em tempo real com o sistema central;
- Dificuldade em alcançar o parecer positivo da Comissão Nacional de Protecção de Dados na armazenagem biometrica.

BIOMETRIA COM SMART-CARD

Um outro modelo é proposto envolvendo o melhor da biometria e dos *smart cards*. O código PIN necessário para autenticar os *smart cards* é substituído por uma característica do indivíduo.

A abordagem de segurança é feita através de algo que temos – o *smart card* – e algo que somos – característica biometrica. A base de dados guarda apenas o resultado da combinação da informação biometrica do indivíduo com um padrão aleatório armazenado no cartão. Quando o indivíduo necessitar de se identificar, apresentará o cartão e disporá a característica física usada no sistema. A combinação do padrão memorizado no cartão e a característica biometrica será então cruzada com a informação arquivada na base de dados. Em caso de igualdade, é assumida a autenticidade da identidade. A memória do cartão contém ainda as chaves privadas que permitem a assinatura digital do indivíduo.

As principais vantagens associadas a este tipo de iniciativa envolvem:

- A não arquivamento de informação biometrica;
- A **insuficiência do cartão para autenticar** a identidade, descartando a possibilidade de roubo ou partilha de identidade;
- A inexistência de um código PIN a memorizar;

- A baixa taxa de repúdio;

O diagrama representado na Figura 4-10 esquematiza o processo de registo, bem como o de autenticação em momentos posteriores.

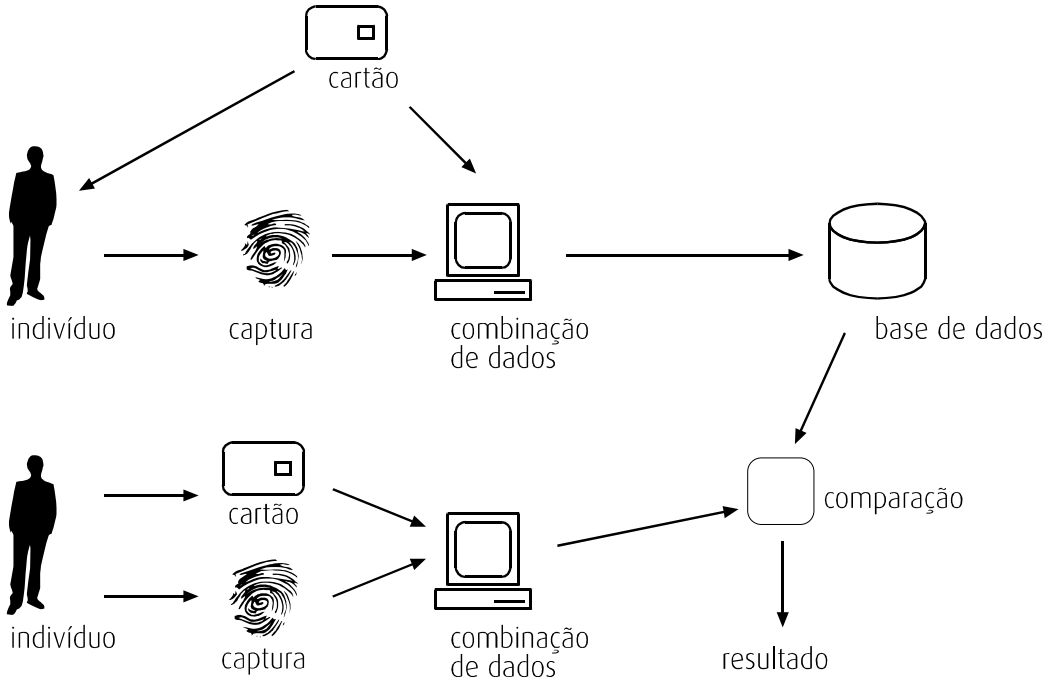

Figura 4-10 Arquitectura de identificação partilhada biometria e Smart-Card[20]

Por outro lado, existem alguns contras que condicionam a adopção deste modelo, como por exemplo:

- O elevado custo associado à dupla infra-estrutura de leitura biometrica e do smart-card;
- A dependência da comunicação em tempo real com o sistema central;
- A perda do cartão impossibilita a identificação e autenticação do sujeito.

[20] Modelo adaptado do proposto por Gelbord e Roelofsen

4.4. DESENVOLVIMENTO E IMPLEMENTAÇÃO DO PROJECTO

O desenvolvimento de sistemas de informação envolve as redes de comunicação, o desenvolvimento de aplicações, a adaptação dos sistemas já existentes e poderá ser realizado recorrendo a dois paradigmas, o desenvolvimento interno e o *outsourcing*.

No caso do desenvolvimento interno, as instituições usam os seus próprios recursos – humanos e técnicos – na prossecução das tarefas associadas às diferentes vertentes do desenvolvimento. Desta forma, é proporcionado um controlo mais eficaz sobre as opções técnicas, bem como sobre a funcionalidade das aplicações.

Por seu lado, o *outsourcing* caracteriza-se pela delegação em empresas terceiras de um conjunto de serviços associados ao sistema de informação. Desta forma, aqueles que sub contratam – no caso em estudo, as autarquias – conseguem um maior controlo dos custos operacionais, eventualmente reduzindo custos, tendo um acesso privilegiado ao conhecimento sem necessitarem de contratar ou locar recursos humanos. Assim, as organizações poderão concentrar os seus esforços nas actividades principais.

4.4.1. Ciclo de vida do projecto

O processo de desenvolvimento da miríade das tecnologias ocorre através de ciclos iterativos que permitem o afinar das mesmas em cada uma das passagens do ciclo.

Os ciclos iterativos permitem um desenvolvimento incremental de tal forma que num curto espaço de tempo existirá um protótipo rudimentar. Este será submetido a uma avaliação – nas fases inicias, a avaliação será realizada por grupos de controlo de qualidade e, nas fases mais avançadas, por grupos de utilizadores piloto, seleccionados de entre a população alvo final – onde serão apontadas deficiências que levarão a um novo ciclo de desenvolvimento. Este ciclo terá fim quando a versão apresentada demonstre robustez, fiabilidade e atinja os objectivos propostos. Antes da tecnologia estar totalmente terminada, inicia-se o processo de

transferência de tecnologia, que visa transferi-la da equipa de desenvolvimento para as equipas que irão implementá-la na prática.

A Figura 4-11 ajuda a perceber os ciclos iterativos no desenvolvimento de tecnologias.

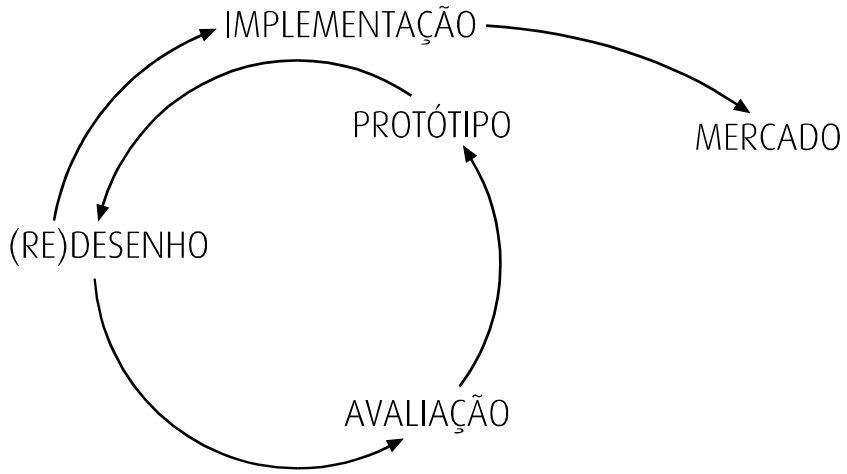

Figura 4-11 Ciclo iterativo de desenvolvimento

4.5. APLICAÇÃO PRÁTICA

No âmbito da gestão da identificação desenvolvem-se interacções entre os diferentes actores do sistema. Neste caso específico, os relacionamentos ocorrem entre os munícipes, a Administração Pública local, as empresas municipais e as empresas privadas tendo um denominador comum, identificável por todos. Este denominador é o número único de identificação municipal. Este número será o garante de que todas as entidades reconhecerão o indivíduo enquanto tal, pelo que as organizações deverão adaptar os seus sistemas de forma a incorporarem esta informação transversal. Estas adaptações poderão ser atenuadas recorrendo a uma tabela de conversão entre a referência interna do indivíduo e o número único de identificação municipal.

O artigo 35º "Utilização da Informática" da Constituição da Republica Portuguesa diz no seu 5º ponto que: "É proibida a atribuição de um número nacional

único aos cidadãos". No entanto, e dado o contexto local, a aplicação do número único de identificação municipal não se reveste de inconstitucionalidade. Este número será único na sua identificação em qualquer organização do sistema – ainda que com tabelas de conversão interna, como já referido. Ou seja, o munícipe número 1234567 será reconhecido como o mesmo indivíduo num departamento municipal, numa empresa pública, ou numa empresa privada – desde que associada ao sistema.

Daqui decorre um conceito fundamental intimamente relacionado com as diferentes organizações do sistema: o contexto. A gestão da identificação do munícipe ocorre num ambiente intercontextual onde é mantida a confidencialidade das informações que dizem respeito a apenas um contexto. Isto é, a informação que apenas diz respeito a determinado contexto é somente acessível do seu interior, estando o acesso restrito a outras fontes. Todavia, a implementação de um sistema de gestão da identificação do munícipe apenas se torna justificável quando se procura a desburocratização. Neste sentido, as trocas laterais de informação – entre organizações parceiras – desempenham um papel fundamental. Estas trocas devem estar asseguradas pela interoperabilidade semântica dos sistemas vigentes nas partes. Níveis superiores de interoperabilidade são atingidos recorrendo a mapas de conversão da informação, onde esta informação, detida por uma das partes, é partilhada assumindo novos formatos, de forma a potenciar o seu valor para a parte receptora. Os contextos enaltecem a pertinência da existência de um identificador único na identificação dos munícipes. Será este número que relacionará todas as trocas de informação entre os organismos.

As organizações privilegiam o acesso a informações provenientes de fontes autenticas, isto é, onde esta é gerada. De forma análoga, na gestão da identificação dos munícipes, as entidades procuram aceder a fontes autênticas de informação. Estas fontes autênticas caracterizam-se pela sua fiabilidade e obedecem a regras rígidas:

- A informação presente numa fonte autêntica é tida como correcta;
- A informação presente numa fonte autêntica é recolhida apenas uma vez;

- A informação presente numa fonte autêntica é reutilizada sempre que possível.

Partindo de um caso genérico, a Figura 4-12 simplifica o processo de interoperabilidade entre dois diferentes contextos. Neste caso, um serviço público e uma empresa municipal, mas o conceito deverá ser extrapolado a outras relações.

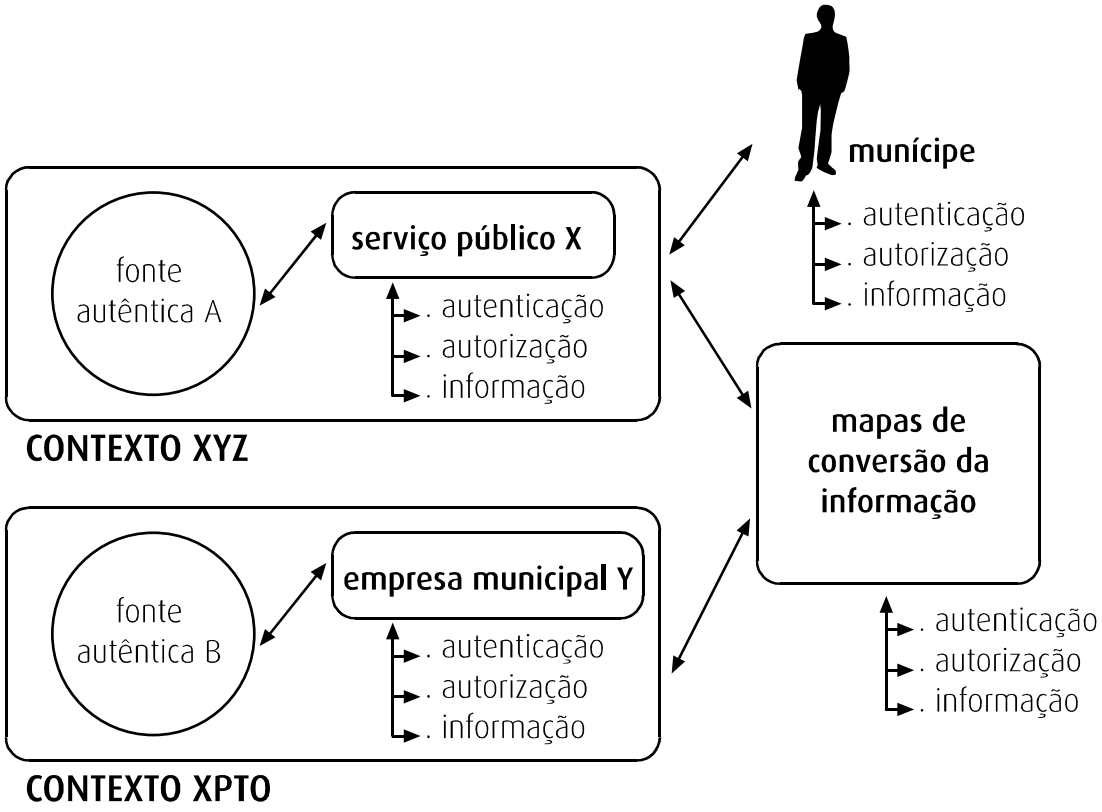

Figura 4-12 Interoperabilidade entre contextos[21]

A aplicação prática da gestão da identificação do munícipe requer um sistema de identificação e autenticação centralizado, transversal e deverá envolver todas as dimensões da Administração Pública local. A presente proposta assenta então, na criação um sistema integrado de identificação tendo como horizonte o local.

[21] Adaptado da proposta da Modinis IDM (2005)

4.5.1. Perspectiva do munícipe

Com a implementação da gestão da identificação individual, os munícipes fruirão da aproximação no relacionamento com as entidades existentes no território em que habitam. Essa aproximação será realizada em quatro vectores chave: a identificação, a autenticação, a participação e, por fim, o financeiro.

As características associadas ao vector da identificação são manifestas. A transversalidade da gestão da identificação permite que o munícipe seja reconhecido como a mesma entidade em todas as dependências municipais e empresas privadas que façam parte do projecto. O uso de *smart cards* personalizados tem vantagens associadas no caso da identificação sem recurso a tecnologias digitais. De facto, a personalização do cartão envolve a incorporação de informação identificativa pessoal impressa na superfície do cartão, permitindo comprovar a identidade do munícipe por observação directa.

Por outro lado, e recorrendo a infra-estruturas de chaves públicas – as já referidas PKI –, a gestão da identificação permite autenticar a identidade do munícipe em diferentes sistemas, assegurando, por exemplo, o acesso a serviços recorrendo à Internet ou a autenticação de documentos. A gestão da identificação tem também impacto sobre a participação dos munícipes. De facto, a concentração num único *token* facilita a predisposição para a mobilização social. No caso dos referendos locais, o sistema adoptado para a gestão da identificação facilita a participação ao desprender-se, por um lado, do cartão de eleitor e, por outro, ao confirmar que aquele cidadão pertence ao território.

Por fim, este modelo permite criar uma espécie de sistema "via verde" nos pagamentos dos serviços utilizados. Os modelos de pagamento serão discutidos adiante. No entanto, fica já patente a valência financeira. Esta permite a desmaterialização do uso de dinheiro no pagamento de serviços, a possibilidade de liquidação no local, sendo desnecessária a deslocação à tesouraria, quantas vezes deslocada fisicamente e a emissão de uma factura mensal detalhada de todos os serviços usufruídos. As facturas serão emitidas pelas entidades que facultam os serviços e incluirão os serviços prestados, que poderão ser tão diversos como por exemplo:

- As taxas municipais;
- Os licenciamentos para construção, de publicidade e outros;
- O estacionamento, quer de rua, quer em espaços públicos, bem como ainda a eventual integração de espaços privados[22];
- O uso de transportes públicos, podendo inclusive a actuação do município como integrador de diferentes entidades de transportes, inclusive empresas de índole privada;
- O uso de equipamentos desportivos municipais, como o caso de piscinas ou ginásios;
- O acesso a equipamentos sócio culturais como feiras, teatros ou museus;
- Enfim, todas as interacções financeiras que se possam dar entre o munícipe e as diferentes entidades.

[22] A empresa Via Verde está a preparar um projecto, a iniciar durante o segundo semestre de 2006 que permite o pagamento do estacionamento de rua. Para mais informações ver a entrevista no Anexo D: Entrevista com Eng. Paulo Marques, Director técnico da empresa Via Verde Portugal – Gestão de Sistemas Electrónicos de Cobrança, SA.

O resumo transcrito na Figura 4-13 permite rapidamente consultar as vantagens associadas à gestão integrada da identificação sob o ponto de vista do munícipe.

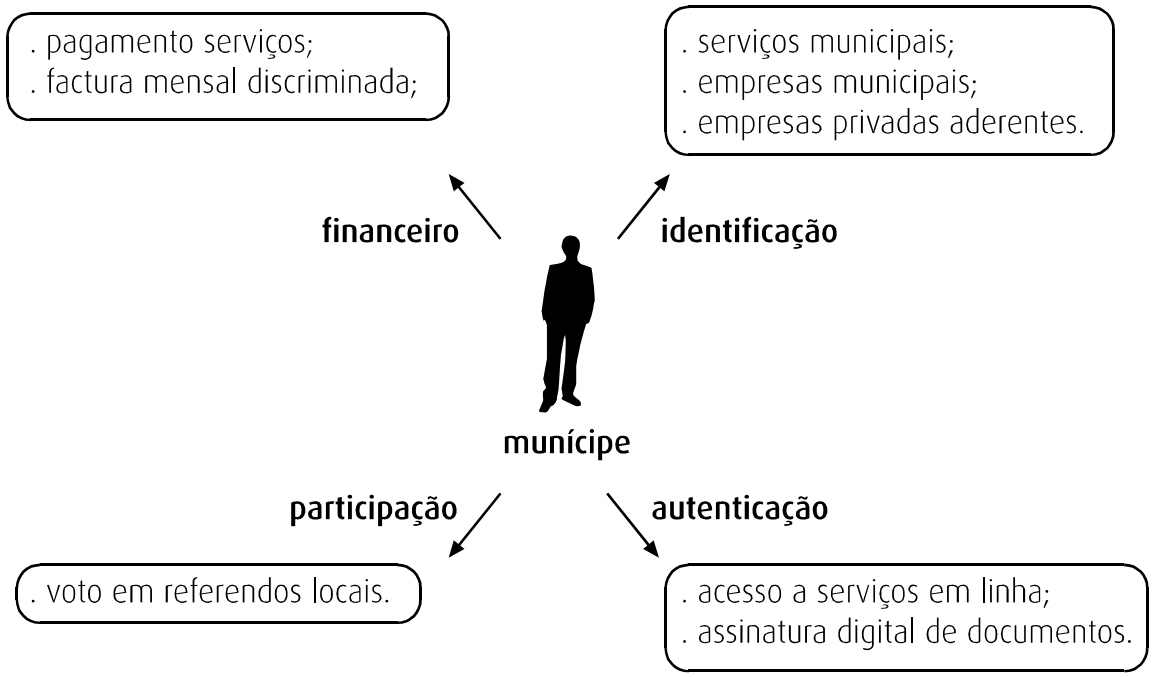

Figura 4-13 A Gestão da Identificação na perspectiva do munícipe

4.5.2. Perspectiva dos órgãos municipais

As autarquias, nomeadamente os diversos serviços, bem como as suas empresas municipais, poderão tirar partido da iniciativa de gestão da identificação dos seus munícipes. Estas valias traduzem-se em quatro eixos: identificação, financeiro, controlo e relacionamento.

A identificação, em associação com a autenticidade da identidade, permite traçar um perfil integrado do munícipe. Os órgãos municipais poderão relacionar informações provenientes dos seus diferentes serviços e obter, desta forma, um conhecimento mais profundo sobre todos e cada um dos seus munícipes. Independentemente das propostas tecnológicas apresentadas, a gestão da identificação dos munícipes permite que estes rapidamente se identifiquem junto dos serviços. É ainda possível o rápido preenchimento dos cabeçalhos dos

formulários, onde constam os dados pessoais do indivíduo, contribuindo para a celeridade do atendimento público.

A nova forma de pagamento de taxas e serviços municipais contribui para a simplificação da tesouraria municipal[23]. Uma vez que as transacções são electrónicas, não é necessário a existência de dinheiro trocado em caixa. Por outro lado, permite locar as pessoas noutras tarefas de valor mais produtivo para o município. A emissão da factura única mensal das taxas e serviços prestados promove, numa perspectiva da responsabilidade social, o uso racional do papel, mas promove também, o agilizar contabilístico, concentrando num único registo um conjunto alargado de elementos.

A gestão da identificação permite não só cuidar dos relacionamentos com os munícipes, mas também com os funcionários públicos. Este relacionamento envolve um controlo efectivo sobre os funcionários, gerindo o acesso físico a determinados espaços do município, bem como o acesso lógico aos terminais informáticos. Em ambos os casos, obede a critérios rigorosos de segurança que envolvem métricas, como por exemplo, níveis de controlo de acesso enquadrados no plano de segurança. Estes níveis identificam o perfil de utilizador e consentem poderes diferenciados.

O potencial do controlo por parte dos órgãos municipais estende-se também na fiscalização. Será possível, por exemplo, aos agentes fiscais rapidamente consultarem o estado das licenças camarárias – se foi efectuado algum pedido de licenciamento, se este foi deferido, ou se por contrário, foi indeferido – e verificarem ainda o estado dos pagamentos das taxas.

No eixo do relacionamento, a gestão da identificação contribuiu inequivocamente para a aquisição de informações sobre os munícipes que servirão de suporte às estratégias de relacionamento[24], entre outras, suportará estratégias

[23] Os munícipes poderão continuar a usar os métodos tradicionais de pagamento, não sendo exclusivos os métodos de pagamento adiante propostos

[24] Ou CzRM, Citizen Relationship Management

de marketing. Por fim, o município beneficiará da gestão da identificação na participação através dos votos. A tecnologia de suporte à gestão da identificação elimina a necessidade de recurso ao cartão de eleitor, ou outros meios, para efectuar referendos locais. O sistema de gestão da identificação do munícipe é o garante da residência do indivíduo no território.

A Figura 4-14 simplifica a concepção do impacto da gestão da identificação na óptica do município e das empresas municipais.

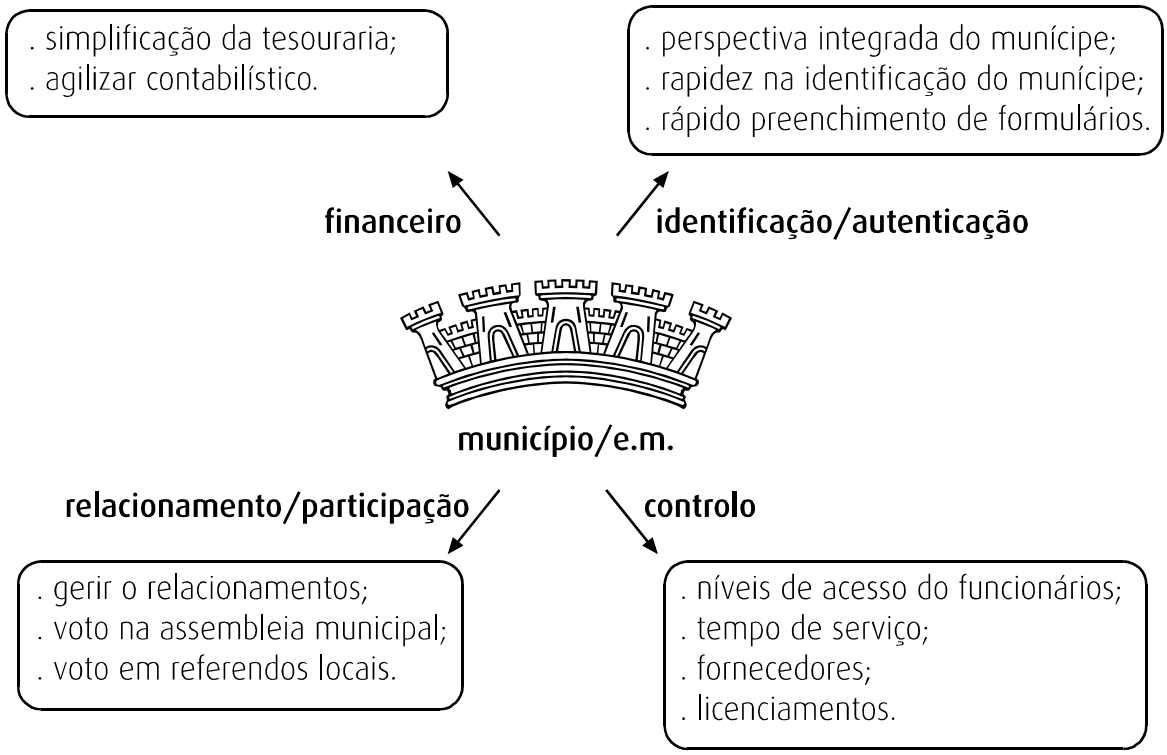

Figura 4-14 Perspectiva do município e empresas municipais

4.5.3. Perspectiva do sector privado

Os proveitos que as empresas do sector privado obtêm na adesão ao sistema de gestão de identificação do munícipe estão em larga medida relacionados com a identificação e autenticação do indivíduo. Baseadas na fidelidade da infra-estrutura do projecto, as empresas privadas beneficiam da veracidade dos dados pessoais apresentados pelos seus clientes, não sendo necessário formas suplementares de verificação. O sistema de gestão da identificação dos munícipes permite

rapidamente identificar os clientes com os principais dados, nomeadamente: o nome, a morada, e os contactos, sendo possível, de forma análoga aos serviços municipais, o rápido preenchimento dos cabeçalhos dos formulários.

Os potenciais benefícios que possam advir para as organizações privadas, resultantes da sua efectiva adesão, serão amplificados numa perspectiva de *cluster*. Paradoxalmente, quanto maior for a oferta de um dado serviço, ou seja, o número de concorrentes; maior será a receptividade dos munícipes. Imagine-se o caso dos transportes. Existem municípios onde existem diversos actores privados no fornecimento de transportes regulares de passageiros. Os clientes tenderão a seleccionar aquelas empresas que disponibilizem a possibilidade de fruir dos benefícios do sistema de gestão da identificação aos munícipes, nomeadamente, questões relacionadas com o pagamento de serviços. Verifica-se aqui um critério de inclusão, onde aquelas empresas que são exteriores ao sistema terão que apostar noutras formas de fidelização dos seus clientes, no sentido de manter a sua viabilidade económica. Por outro lado, aquelas que estão incluídas no sistema, serão avaliadas segundo outras métricas, como por exemplo, os horários, os trajectos, ou a condição geral das viaturas. Numa outra perspectiva, as empresas poucos benefícios obterão na aposta de fidelização dos seus clientes – neste caso, através de passes.

4.5.4. Formas de pagamento

Uma das grandes vantagens propostas por este modelo de gestão da identificação do munícipe reside no facto deste poder efectuar pagamentos de serviços fruídos no âmbito do território sem necessidade de usar dinheiro – pois por vezes se poderá esquecer dele.

Assim, e baseado nas entrevistas realizadas, são apresentadas três formas de quitação, são elas: os pré pagamentos, o débito directo e o pagamento de baixo valor.

O pré pagamento funciona de forma análoga aos carregamentos dos cartões dos operadores móveis. De forma simples, o munícipe desloca-se a uma caixa ATM e selecciona a opção de pagamentos especiais e credita um determinado valor à

sua escolha no seu *token*. Este saldo, permitirá efectuar o pagamento dos serviços prestados de forma rápida e segura. Esta situação acarreta vantagens óbvias para o município, pois permite fortalecer a liquidez das suas contas com o avanço do dinheiro dos seus munícipes. No entanto, esta solução poderá causar desconforto aos cidadãos, podendo mesmo condicionar a utilização desta valência.

O funcionamento do débito directo é semelhante ao anterior. Ou seja, o munícipe dispõe no seu *token* de determinado saldo que permitirá ir liquidando o pagamento dos serviços. A diferença reside na creditação do saldo. Uma vez atingido o valor mínimo, os serviços municipais contactam directamente o banco do cliente e creditam o *token* com uma verba previamente acordada. Aos anteriores prós e contras, poder-se-á destacar agora a não obrigatoriedade de deslocação à caixa ATM para a creditação do *token*, bem como de portar um cartão Multibanco.

Por seu lado, os pagamentos de baixo valor requerem um intermediário entre o município e o banco do munícipe. Um destes intermediários é a SIBS, pois a transacção não é mais do que a emulação da utilização do cartão Multibanco. Cabe ao município registar o conjunto das interacções com os seus munícipes que recorreram ao *token* para efectuar o pagamento. Periodicamente, e de forma automática, o sistema de informação do município contacta os servidores da SIBS e envia a informação relativa ao valor de cada transacção, bem como o identificador único do munícipe. A SIBS possui uma base de dados que relaciona o identificador único do munícipe e um cartão Multibanco pertencente ao munícipe, transformando a transacção realizada com o *token*, numa operação ocorrida com o cartão Multibanco. Este método de pagamento envolve um maior risco de fuga ao pagamento por parte dos infractores, uma vez que, por exemplo, a validação do saldo da conta para a liquidação do serviço, é realizada em diferido. O município deverá desenvolver mecanismos de recuperação de créditos mal parados, contudo este sistema tem um maior potencial para a adesão.

4.5.5. Herança de valências

Iniciativas como esta que é proposta, requerem enormes investimentos, que contudo, deverão notar racionalidade económica. Nesse sentido, a gestão da

identificação tem potencial para ser implementada tendo em consideração os custos.

Como humanos que são os munícipes, gozam do legado genético próprio da espécie. De entre várias outras características, os seres humanos são uma espécie gregária, ou seja, que se reúne e desenvolve relações entre indivíduos da mesma espécie, constituindo as suas famílias. Se por um lado, os adultos da família são considerados com indivíduos independentes, já a descendência pressupõe dependência directa dos adultos.

A dependência que os descendentes têm, liberta-os de uma série de responsabilidades que serão os seus progenitores a terem que lidar com elas. Assim, as potenciais interacções entre os adultos e as entidades do território serão mais numerosas e mais complexas do que as interacções entre os seus descendentes e as mesmas entidades. Daqui, deduz-se que o nível de segurança necessário para satisfazer as interacções entre os filhos e as entidades será menor do que no caso dos seus pais.

Os jovens tendem a negligenciar responsabilidades e a danificar diversos objectos pessoais – ainda que inadvertidamente. Atendendo a este facto e a que os *smart cards* são mais caros do que qualquer outra forma de cartão, conforme afirma Mike Hendry (1997, p.210), os promotores deverão optar por uma solução mais simples. Por outro lado, a adolescência caracteriza-se por um rápido crescimento, conduzindo, por vezes, a grandes alterações morfológicas num curto espaço de tempo. Neste caso, a identificação baseada em características biometricas poderá também apresentar problemas no seu desempenho.

O compromisso proposto baseia-se na implementação de uma forma simplificada de um cartão de identificação para os filhos, uma espécie de cartão de identificação júnior. Este cartão goza de valências herdadas do meio de identificação de um dos progenitores, funcionando assim, como uma instância do *token* de um dos pais. De forma a simplificar o raciocínio, imagine-se os seguintes casos práticos.

A mãe, usando o seu meio de identificação, liquida a mensalidade relativa ao uso da piscina municipal por parte dos seus filhos. Posteriormente, quando estes se

deslocarem à piscina, os seus cartões serão processados. O sistema irá então verificar se a pessoa progenitora efectuou o pagamento. Estando confirmada a liquidação da mensalidade, será validado o acesso ao equipamento.

Por outro lado, o cartão de identificação júnior poderá ainda ser usado no acesso às refeições nas escolas do primeiro ciclo – que estão a cargo do município. È assim possível aos pais seleccionarem um conjunto de dias em que pretendem que os seus filhos almocem na escola e comodamente efectuarem o pagamento das mesmas. Para além do pagamento das refeições, poderão ainda controlar a efectividade das mesmas. Já na perspectiva do município, o uso do cartão poderá ajudar no controlo do número de refeições fornecidas pelo *catering.*

Os jovens poderão ainda usar o seu cartão no uso dos transportes públicos, beneficiando de descontos decorrentes da sua condição de estudantes.

Estes pagamentos enquadram-se nas formas de pagamento de serviços prestados, discutidas anteriormente.

4.6. RISCOS E AMEAÇAS

Muitos projectos e iniciativas com o sentido de alterar organizações – quer seja ao nível estratégico, operacional ou tecnológico – acabam por fracassar, mesmo em fases de alguma maturidade no desenvolvimento. Os factores que contribuem para esta situação são variados e têm diversas origens. Por isso, os decisores e as equipas de desenvolvimento têm que ter presente esta ameaça de insucesso, devendo agir persistentemente e com elevada capacidade de trabalho, a fim de contrariar todas as adversidades que seguramente surgirão.

Propõe-se o agrupamento das fontes de potenciais riscos em três grupos distintos: os riscos e ameaças que são externos às iniciativas; os que compreendem factores humanos; e as tecnologias.

4.6.1. Factores externos

Numa sociedade habituada a objectivar índices e graus em escalas traduzidas por números e estatísticas, a aferição do grau de confiança do sistema poderá ser uma tarefa demolidora. Por um lado, existem as ameaças associadas às tecnologias adoptadas. Por outro, os utilizadores poderão exercer um uso potencialmente nocivo. A identificação individual no contexto da gestão da informação municipal, pelo seu carácter essencial, é altamente dependente da confiança que transmite.

Miguel Teixeira (2003, p.280) realça o aumento de capacidade de iniciativa e intervenção do sector privado em relação ao público. Esta situação conduz ao acentuar do desnivelamento social e da desigualdade territorial associados às infra-estruturas digitais, devido à racionalidade económica das organizações. Esta polarização, para além de indesejável, contribui inequivocamente para a criação de hiatos sociais.

Ao nível legal, é também colocado um desafio baseado na Lei n.º 67/98 de 26 de Outubro, a lei da protecção de dados pessoais, no seu artigo 9.º interconexão de dados pessoais. Para que seja possível a implementação dum plano como o proposto, onde a interdependência e interoperabilidade de sistemas são a sua base, é necessário um parecer positivo da Comissão Nacional de Protecção de Dados.

4.6.2. As organizações e as pessoas

A diferença cultural das organizações e das pessoas que as constituem, associada às diferentes origens sectoriais (público e privado), bem como os diferentes preconceitos, motivações e a identidade corporativa são tendencialmente incompatíveis, levantando sérios problemas de cooperação entre as partes. Também a falta de um recurso de termos devidamente acordados, a fim de facilitar o entendimento das partes, levanta problemas meta linguísticos. Por exemplo, quando se fala do o termo "entidade", este poderá referir-se ao indivíduo sujeito à identificação, o munícipe, ou por outro lado, poderá referir-se à instituição que requereu a identificação do indivíduo. Num esforço de tentar resolver este

problema, a Comissão Europeia formulou uma proposta para estabilizar os termos comuns, que poderá ser encontrada[25] no Anexo A: Proposta da Comissão Europeia para a terminologia comum no contexto da gestão da identificação electrónica.

As falhas de comunicação apresentam problemas ainda mais graves quando, por exemplo, um ou mais organismos se atrasam em relação a outros na implementação dos seus sistemas. A consequência directa do eventual desajuste temporal é a perda do efeito surpresa que permitiria um arranque mais notório por parte da comunidade. Por outro lado, estes desajustes poderão condicionar o desempenho daqueles que cumpriram os prazos. Cabe à comissão coordenadora do projecto zelar pelo cumprimento dos prazos, assim como pela cooperação efectiva das partes.

A burocracia e os interesses instalados poderão ser outra força bloqueadora da inovação organizacional. Pela imparcialidade das tecnologias, estas inibem eventuais tentativas de contornar os procedimentos legais, absorvendo o estatuto dos indivíduos infractores, bem como o carácter arbitrário de algumas decisões.

O uso das TIC é um meio privilegiado que promove a intensificação da criação e da partilha de informação. O crescimento deste capital poderá contribuir para a asfixia de absorção, causada pelo excesso de informação. Numa perspectiva interessante, Richard Wurman (2001) afirma que não tem ocorrido uma explosão de informação, mas antes uma explosão de não informação ou de informação que simplesmente não informa. Actualmente, tão importante como ter acesso à informação, é a forma como ela está apresentada e organizada. É fundamental ter mecanismos que permitam procurar, classificar, organizar e imprimir a informação à medida das necessidades de cada indivíduo. O excesso de informação leva à ansiedade, à confusão, à incompreensão e a uma espiral depressiva que invalida a possibilidade de poder assimilar qualquer informação potencialmente importante. Não é preciso ser detentor de toda a informação disponível para tomar uma boa decisão. Na verdade, são muitas as decisões tomadas baseadas em informações

[25] A versão mais recente do documento é a v2.01. As actualizações encontram-se em https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc

incompletas. O real valor da informação não está na sua capacidade de decidir – de facto a informação *de per si* não decide – mas sim na sua exactidão e na compreensibilidade intrínseca.

Wurman refere ainda a sedução como um meio para comunicar mais eficazmente. Aliás, esta é a estratégia adoptada pelos publicitários com a finalidade de promover os seus clientes perante a sociedade. De forma análoga, a informação deverá ser apresentada de forma "sexy", que atraia e seduza todos aqueles que acedem à mesma. A interface da informação deve traduzir os seus conteúdos (informação) de forma inteligível ao utilizador, para que os mesmos tenham valor por si e ajude o utilizador a tomar decisões. Estas preocupações estéticas não pretendem retirar valor ao conteúdo, mas sim exprimi-lo, com vista a potenciar a sua interpretação.

4.6.3. Tecnologias

Um dos principais problemas dos sistemas de identificação encontra-se no facto de não existir uma tecnologia amplamente aceite como normativa. São propostas diferentes tecnologias, de onde se destacam os *smart cards,* bem como a biometria, vislumbrando-se como sendo os casos mais aptos para este tipo de aplicação. Ainda assim, mesmo dentro destas tecnologias não existe um consenso, havendo uma disputa de oferta alargada, onde existe um mercado concorrencial com diferentes soluções propostas, tornando difícil a selecção da ideal. A este facto junta-se ainda o carácter volátil das soluções, uma vez que se encontram em constantes evoluções – quer seja ao nível da capacidade de informação, quer de processamento ou de novas normas de segurança – apresentando-se como soluções de termo incerto. As tecnologias actuais servem, por isso, necessidades a médio prazo, pelo que, actualizações ao nível das tecnologias de tempos a tempos, devem estar previstas à partida pelos decisores.

Por outro lado, é muito provável que existam incompatibilidades entre os sistemas informáticos – o formato dos dados, os protocolos de comunicação, as medidas de segurança, e outros – usados pelos diferentes departamentos municipais e as empresas que participam no sistema.

Tornar os sistemas compatíveis entre si é um enorme desafio, não só por razões técnicas, mas também pela provável vulnerabilidade, causada pelas tecnologias de suporte à comunicação necessárias à interdependência e à interoperabilidade dos mesmos. As redes de comunicação, nomeadamente a Internet, têm fragilidades que lhes são próprias. Para além das causas físicas naturais – inundações, terramotos – existem debilidades lógicas associadas a ataques de diversas origens onde, uma vez violada a infra-estrutura de segurança, poderão se alastrem por todo o sistema.

4.7. SUMÁRIO

Este capítulo incidiu sobretudo na discussão de um modelo de identificação individual, cuja finalidade encerra a satisfação das necessidades dos munícipes, da Administração Pública local, das empresas municipais e das empresas privadas aderentes, através de um processo simples e seguro. Todavia, considerando todas as mudanças que esta abordagem obriga. Assim, foram apresentadas três propostas relativamente aos identificadores *(tokens)*, onde foram discutidos os processos de implementação, bem como as suas vantagens e desvantagens.

Discutiu-se a implementação e a aplicação destas tecnologias numa perspectiva mais prática, tendo sido explorados alguns cenários, baseados em propostas disponíveis no mercado. Foram também consideradas as principais perspectivas das partes, nomeadamente as principais vantagens que lhes são afectas. Os principais riscos e ameaças que normalmente se associam a projectos deste enquadramento e dimensão foram também abordados.

A proposta realizada tem por objectivo sensibilizar os diferentes actores (os políticos, a administração pública e a sociedade em geral) para um conjunto de questões associadas à identificação dos munícipes. Em última instância, esta proposta oferece aos munícipes, uma cidadania mais prática, logo menos burocrática, contribuindo para a melhoria da qualidade de vida das populações actuais e futuras.

5 CONCLUSÕES

A Humanidade estará porventura a experimentar o mais intenso período de revoluções sócio culturais, também induzidas pela tecnologia de informação. A envolvente impõe mudanças de paradigma, com claras aspirações de melhoria dos índices de produtividade e competitividade, que têm provocado profundas alterações nos relacionamentos entre as pessoas e, entre estas e as organizações. Tem-se assistido à desmaterialização da presença humana nos relacionamentos, uma vez que estes se desenvolvem cada vez mais no digital, beneficiando da sua principal virtude: a ubiquidade.

Actualmente, é ainda possível encontrar departamentos e organizações isoladas, as denominadas ilhas de informação (Luís Gouveia 2004, p.40), onde há lacunas na satisfação das necessidades de informação. Estes problemas estão associados à falta de coordenação de esforços e de percepções desajustadas quanto

às necessidades de informação. É necessário desenvolverem-se esforços no sentido de integrar estas ilhas num espaço alargado de partilha de informação.

Relembrando os objectivos da dissertação, poder-se-á constatar que a finalidade última deste trabalho é prestar um contributo para uma proposta de um modelo para a gestão da identificação dos munícipes no contexto das autarquias. Ao longo do trabalho foram dissecados diversos assuntos relacionados com o tema. Houve um primeiro enquadramento do tema num contexto mais alargado que envolve a cidadania e os governos electrónicos. Mas, mais do que isso, a sua contextualização na sociedade da informação. Partiu-se depois para o enquadramento do trabalho na gestão da informação, num sentido mais lato.

Como já referido, a agitação em torno destas temáticas é enorme, não só nas iniciativas visíveis pelas massas, mas também nos bastidores, onde são geradas essas iniciativas. Estas fontes geradoras têm origens em diferentes referenciais, desde iniciativas ao nível local e das regiões, passando por orientações ao nível dos países – como o caso do plano tecnológico promovido pelo actual governo português – até às directivas de nível comunitário. Foram observadas as considerações destes esforços, tentando retirar destes o melhor contributo para este trabalho.

Num plano mais próximo do objecto de estudo, foram analisados os requisitos estratégicos, operacionais, tecnológicos, sociais, legislativos, deontológicos e económicos que orientam os sistemas de identificação, com o intuito de garantir as mais elementares condições para o sucesso da sua implementação.

Em última instância foi manifestada a tentativa de – integrando todas as considerações prévias – materializar o contributo para a proposta dum modelo para a gestão da identificação do munícipe numa perspectiva mais prática. Nesta fase, foram apresentadas diferentes soluções tecnologias disponíveis no mercado, analisando as suas virtudes e principais deficiências, deixando em aberto a tomada de decisão sobre a adopção de qualquer um dos cenários apresentados.

O conjunto das diversas entrevistas realizadas, associadas com a maturidade do mercado na área dos sistemas de identificação, contribuíram de forma significativa para o desenrolar do estudo.

No desenrolar da dissertação, foi sempre mantido o alto grau de abstracção por dois motivos:

- O âmbito genérico da dissertação permitirá a sua adaptação à realidade de cada autarquia;
- A incapacidade humana para lidar com todas as implicações de um projecto desta dimensão, sendo necessária uma equipa multidisciplinar, tendo sido escolhida uma abordagem orientada para a Gestão da Informação que permite informar projectos específicos.

Apesar de todas as dificuldades e desafios a superar, novas cidades digitais são desenvolvidas. É um facto que é com os erros que crescemos intelectualmente, se deles conseguirmos tirar frutos das reflexões posteriores. Não devemos por isso ter receio em transformar átomos em bits[26]. Devemos sim aproximar as tecnologias às pessoas, experimentar e aprender.

São as sociedades abertas que podem fruir das inovações adoptadas no seu seio. Esta dinâmica requer audácia, pois existem riscos a correr. Contudo, deve estar sempre presente o objectivo último destas iniciativas: a melhoria da qualidade de vida das populações.

5.1. INOVAÇÃO NOS SERVIÇOS MUNICIPAIS

> *"...one of the main contributions of Europe in the 21st century will be the new model of its ancient and modern cities: cities, which are truly connected, which are innovative and*

[26] No seu livro "Being Digital", Nicholas Negroponte (1995) faz uma interessante analogia entre o analógico e o digital, ou os átomos e os bits.

productive, creative in science, culture, and ideas, whilst maintaining decent living and working conditions for their people; cities, which will connect the past with the future, through a vital and vibrant present."

European Council Town Planners (2003, p.10)

A inovação é sem dúvida um aliado na integração de esforços municipais, de empresas, munícipes/clientes e porque não, países, gerando valor para todas as partes envolvidas. Estas inovações não se devem concentrar apenas na tecnologia – se bem que este seja um vector importante – mas também nos procedimentos do quotidiano.

O real impacto das estratégias de desenvolvimento inovadoras que frequentemente surgem é inestimável. Apenas a assumpção do risco poderá, com o tempo, responder às actuais dúvidas. Este risco não é mais do que o resultado da "destruição criativa" de Shumpeter, um processo que obriga a repensar todas as linhas orientadoras dos sistemas vigentes.

Hargadon (2003, p.31), baseado nas observações que fez ao trabalho de Tomas Edison escreveu que a *"Innovation is a process of taking apart and reassembling these elements"* – pessoas, ideias e objectos – *"in new combinations"*. Partindo deste pressuposto, e adaptando-o ao objecto de estudo, poder-se-á extrapolar que as autarquias devem estar atentas às iniciativas inovadoras. A adopção de ideias aplicadas noutros cenários, recorrendo à manipulação de objectos com novas formas, ambos integrados por pessoas de diferentes origens, traduz-se em iniciativas percursoras de novos paradigmas, que transformam as autarquias em novos locais para estar.

As fragilidades inerentes às tecnologias podem ser constrangedoras do desenvolvimento potencialmente espectável. Todavia, a existência de plataformas que suportem a informação e o conhecimento, no contexto local, proporciona vantagens competitivas para as regiões.

5.2. PESSOAS E COMPETÊNCIAS

Neste cenário de mudança, o factor crítico de sucesso é sem dúvida as pessoas. A alteração de processos, de estruturas e de tecnologias obriga a uma maior capacidade de adaptação por parte dos recursos humanos das autarquias. Novos indicadores de desenvolvimento emergem; as tradicionais taxas de crescimento, de desemprego, a densidade populacional estão, cada vez mais, desactualizadas. A inovação, a qualificação das pessoas, a flexibilidade e integração das organizações públicas e privadas, a capacidade tecnológica e de iniciativa, são os novos padrões.

Dever-se-á então privilegiar uma maior autonomia e flexibilidade das pessoas e dos próprios órgãos administrativos, onde a atribuição de responsabilidades assume um papel elementar. Sabe-se, no entanto, que nem todas as organizações dispõem de capital humano com estas características. Por isso, as autarquias deverão apostar na qualificação e valorização de competências dos seus colaborares, de forma a potenciar a receptividade aos cenários de mudança. As pessoas deverão consciencializar-se que a mudança tem em vista – ainda que nem sempre verificável na prática – a melhoria da produtividade, através de uma maior eficácia e eficiência no desempenho das funções.

Em linhas com estas reflexões, André Alves (2004, p.13) defende que o "*acréscimo de flexibilidade e autonomia que, por sua vez, só poderá ser concretizado através de um reforçado empenho e exigência na formação e qualificação dos agentes da Administração Pública. No que toca ao governo electrónico, essa formação não passa apenas pela capacidade de utilizar eficazmente as novas tecnologias e pela reconversão profissional mas também pela potenciação de capacidades de adaptação à mudança, de avaliação do desempenho dos serviços e de procura activa de novas formas de conceber e executar os serviços públicos.*"

5.3. DESENVOLVIMENTO ULTERIOR

A maior insuficiência desta proposta está relacionada com a inexistência da aplicação prática que permitiria a verificação de todos os pressupostos conceptuais apresentados. Na verdade, apenas só com vontade política é que será possível continuar a desenvolver o projecto, ou seja, o suporte de um governo local torna-se fundamental.

A aplicação prática da proposta poderá despoletar novos caminhos de desenvolvimento, nomeadamente o alargamento das valências proporcionadas pelo sistema. Por outro lado, e dadas as iniciativas neste contexto a nível europeu, que contudo, ainda não se encontram estabilizadas, a aplicação do modelo deverá ter em vista um certo grau de abstracção, de forma a tornar possível uma posterior integração do sistema de identificação municipal no sistema mais alargado a nível europeu.

Por fim, e num cenário hipotético de desenvolvimento da proposta, é defendida a assimilação de saberes provenientes de diferentes áreas do conhecimento, traduzindo-se na criação de uma equipa pluridisciplinar de desenvolvimento do projecto, que assegure o uso de todo o potencial da oferta tecnológica para o bem-estar do ser humano.

BIBLIOGRAFIA

ALTERMAN, Anton (2003). "A piece of yourself: Ethical issues in biometric identification". *in* Ethics and Information Technology p.139-150. Netherlands: Kluwer Academic Publishers.

ALVES, André; MOREIRA, José (2004). "Cidadania Digital e Democracia Electrónica". Porto: SPI.

BILHIM, João (2004). "A Governação nas Autarquias Locais". Porto: SPI.

CANOTILHO, J. J. Gomes; MOREIRA, Vital (1998). "Constituição da República Portuguesa". Quinta edição. Coimbra: Coimbra Editora.

CUNHA, Miguel et. al. (2003). "Manual de Comportamento Organizacional e Gestão". Segunda Edição. Lisboa: Editora RH.

Daon (2003). "Biometrics and PKI based Digital Signatures: A Short White Paper".http://www.daon.com/downloads/publications/daon_white_paper_biometrics_pki.pdf

DRUCKER, Peter. (2005). "Diário de Peter Drucker". Lisboa: Actual Editora.

eGovernment Unit, DG Information Society, European Commission. "Common Terminological Framework to Interoperable Electronic Identity Management: Consultant paper v2.01". Última actualização 23.11.05. https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf

eGovernment Unit, DG Information Society, European Commission. "Modinis Study on Identity Management in eGovernment". Última actualização 28.02.06. https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/WebHome/Modinis_Problem_analysis_Overview_1.0.pdf

eMayor (2006). "eMayor Project: Creating secure Web services for small and medium sized Government Organisations (SMGOs)". http://www.emayor.org/

Europe's Information Society (2005a). "eEurope 2005: e-Government". Última actualização 31.05.2005
http://europa.eu.int/information_society/eeurope/2005/all_about/egovernment/index_en.htm

Europe's Information Society (2005b). "eEurope 2005: e-Inclusion". Última actualização 31.05.2005
http://europa.eu.int/information_society/eeurope/2005/all_about/einclusion/index_en.htm

Europe's Information Society (2005c). "Identity Management in eGovernment". Última actualização 08.11.2005
http://europa.eu.int/information_society/activities/egovernment_research/focus/identity_management/index_en.htm

Europe's Information Society (2005d). "Regional and local aspects of eGovernment". Última actualização 20.03.2006
http://europa.eu.int/information_society/activities/egovernment_research/focus/regional/index_en.htm

Europe's Information Society (2005e). "The modernisation of public administrations". Última actualização 20.03.2006
http://europa.eu.int/information_society/activities/egovernment_research/focus/modernisation/index_en.htm

European Commission (2006). "eGovernment: Commission calls for ambitious objectives in the EU for 2010". Última actualização 25.04.06
http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/06/523&format=HTML&aged=0&language=EN&guiLanguage=en

European Council of Town Planners (2003). "The new charter of Athens 2003: Vision for cities in the 21st century". Última actualização 20.11.03. http://www.ceu-ectp.org/e/athens/charter2003.pdf

GELBORD, Boaz; ROELOFSEN, Gert (S/D). "A Solution to Privacy Issues in the Use of Biometrics in PKI". http://www.iris.re.kr/iwap01/program/download/g05_paper.pdf

GOUVEIA, Feliz Ribeiro (2003). "Gestão da Informação" *in* Luís Borges Gouveia (Org.), "Cidades e Regiões Digitais: impacte nas cidades e nas pessoas". Porto: Universidade Fernando Pessoa.

GOUVEIA, Luís Borges (2004). "Local e-Government: a Governação Digital na Autarquia". Porto: SPI.

GOUVEIA, Luís Borges e GOUVEIA, Joaquim Borges (2003). "Autarquias Digitais: promessas e desafios" *in* Luís Borges Gouveia (Org.), Cidades e Regiões Digitais: impacte nas cidades e nas pessoas". Porto: Universidade Fernando Pessoa.

GOUVEIA, Luís Borges, Org. (2003). "Cidades e Regiões Digitais: impacte nas cidades e nas pessoas". Porto: Universidade Fernando Pessoa.

GOUVEIA, Luís Borges; RANITO, João (2004). "Sistemas de Informação de apoio à Gestão". Porto: SPI.

Guide (S/D). "Creating a European Identity Management Architecture for eGovernment". http://istrg.som.surrey.ac.uk/projects/guide/

HARGADON, Andrew (2003). "How Breakthroughs Happen: The Surprising Truth About How Companies Innovate". Boston: Harvard Business School Press.

HENDRY, Mike (1997). "Smart Card Security and Applications". Norwood: Artech House, Inc.

IBBT (2004). "Welcome to the IDEM project site". https://projects.ibbt.be/idem/

Liberty Alliance Project (2004). "Digital Identity Defined". http://www.projectliberty.org/

Ligar Portugal (2005). http://www.ligarportugal.pt/

MAFRA, Francisco; SILVA, J. Amado da (2004). "Planeamento e gestão do território". Porto: SPI.

MAUZY, Jeff; HARRIMAN, Richard (2003). "Creativity, Inc.: Building an inventive organization". Boston: Harvard Business School Press.

Modinis IDM (2005). "Conceptual Framework: About sectors and contexts - cross-context identity management". Última actualização 06.03.06 https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ConceptualFramework

Modinis IDM (2006). "Key issues regarding the implementation of pan-European IDM". Última actualização 31.01.06 https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/KeyIssues

MUELLER, Manfred (2004). "Smart card readers bring security online in Germany" *in* Card Technology Today.

NEGROPONTE, Nicholas (1995). "Being digital". New York: Knopf

Observatório da Sociedade da Informação e do Conhecimento (2005). "Governo e Administração Pública". http://www.osic.umic.pt/governo/index.aspx

PATROCÍNIO, Tomás (2003). "Educação e cidadania glocal" *in* Luís Borges Gouveia (Org.), "Cidades e Regiões Digitais: impacte nas cidades e nas pessoas". Porto: Universidade Fernando Pessoa.

PINTO, Ricardo Jorge (2003). "Passar a salto a fronteira electrónica. Estratégias de uso de plataformas digitais nas sociedades analógicas". *in* Luís Borges Gouveia (Org.), "Cidades e Regiões Digitais: impacte nas cidades e nas pessoas". Porto: Universidade Fernando Pessoa.

PORTUGAL (1998). "Lei n.º 42/98 de 6 de Agosto: Lei das Finanças Locais". http://www.dgaa.pt/legis/Diploma.aspx?id=31

PORTUGAL (1999). "Lei n.º 159/99 de 14 de Setembro: Transferência de Competências para as Autarquias Locais". http://www.cm-guimaraes.pt/document/447692/450221.pdf

REGO, Arménio; CUNHA, Miguel Pina (2003). "A Essência da Liderança: Mudança, Resultados, Integridade". Lisboa: Editora RH.

SHEDROFF, Nathan (2001). "An overview of understanding" *in* WURMAN, Richard Saul. "Information Anxiety 2". Indianapolis: Que.

SILVA, J. Amado da (2004). "Empresarialização de serviços – concessões". Porto: SPI.

SILVA, J. Amado da; AMADO, Luís (2004). "Inovação ao serviço das cidades". Porto: SPI.

SILVA, Paulo (2003). "Sistemas de Informação e Cidades Digitais: conceitos e relações" *in* Luís Borges Gouveia (Org.), Cidades e Regiões Digitais: impacte nas cidades e nas pessoas". Porto: Universidade Fernando Pessoa.

STAPE (2006). "Eleição do Presidente da República – 2006". http://www.stape.pt/eleiref/pr2006.htm

TEIXEIRA, Miguel Branco (2003). "O Contexto Territorial no Tempo das Infra-estruturas Digitais" *in* Luís Borges Gouveia (Org.), "Cidades e Regiões Digitais: impacte nas cidades e nas pessoas". Porto: Universidade Fernando Pessoa.

UCMA (2006). "Projecto Pegasus: Relatório Final da Prova de Conceito". Última actualização 07.03.06. http://www.cartaodocidadao.pt/images/stories/relatorio_prova_conceito.zip

UMIC (S/D). "Fórum para a Sociedade da Informação". http://www.umic.pt/UMIC/SociedadedaInformacao/forum/

UMIC (S/D). "Governo Electrónico: Linhas Estratégicas". http://www.umic.pt/UMIC/GovernoElectronico/LinhasEstrategicas/

UMIC (S/D). "Sociedade da Informação: Linhas Estratégicas". http://www.umic.pt/UMIC/SociedadedaInformacao/LinhasEstrategicas/

Unidade de Coordenação do Plano Tecnológico. (2005) "Sociedade do Conhecimento". http://www.planotecnologico.pt/fileviewer.php?file_id=178

WOODWARD Jr., John D.; ORLANS, Nicholas M.; HIGGIS, Peter T. (2003). "Biometrics: Identity Assurance in the Information Age". Berkeley: McGraw-Hill

WURMAN, Richard Saul (2001). "Information Anxiety 2". Indianapolis: Que.

XAVIER, Jorge; GOUVEIA, Luís Borges; GOUVEIA, Joaquim Borges (2003). "Gaia Global: O Cidadão com umbigo da Cidade Digital" *in* Luís Borges Gouveia (Org.), Cidades e Regiões Digitais: impacte nas cidades e nas pessoas". Porto: Universidade Fernando Pessoa.

ANEXOS

ANEXO A: PROPOSTA DA COMISSÃO EUROPEIA PARA A TERMINOLOGIA COMUM NO CONTEXTO DA GESTÃO DA IDENTIFICAÇÃO ELECTRÓNICA

Prepared for the eGovernment Unit

DG Information Society and Media

European Commission

Modinis Study on Identity Management in eGovernment

Common Terminological Framework for Interoperable Electronic Identity Management

Consultation paper

v2.01

November 23, 2005

eGovernment Unit
DG Information Society and Media
European Commission

K.U.Leuven, Belgium
Lawfort, Belgium
A-SIT, Austria

1. Introduction

This short document attempts to provide a common terminological framework for interoperable identity management in eGovernment. This was identified as a key issue that needs to be resolved during the first Modinis[IDM] Workshop of 4 May 2005 in Leuven; a position which was subsequently supported by the eEurope eGovernment subgroup – Ad hoc group on Identification and Authentication. The initial version was largely written between July 6-15, 2005 by the partners of the MODINIS Study on Identity Management in eGovernment (K.U.Leuven, A-SIT and Lawfort). The document has subsequently been updated, based on feedback from Prime, Belgian Federal ICT Ministry and several Member States representatives.

The terms in this terminology paper have been influenced by the following consulted source materials:

- The final report of the first Modinis[IDM] Workshop of 4 May 2005 in Leuven, including the presentations of Frank Robben and Reinhard Posch.
- The presentations given during the meeting of the eEurope eGovernment subgroup – Ad hoc group on Identification and Authentication on 30 June 2005 in Brussels, by Reinhard Posch and the Modinis[IDM] Study Team (represented by Hans Graux)
- FIDIS D 2.1: Inventory of topics and clusters (and the corresponding WIKI page: http://internal.fidis.net/178.0.html?tx_a1wiki_pi1[keyword]=t2.1%20definition
- PRIME D 14.1.a: Framework V1 (http://www.prime-project.eu.org/public/prime_products/deliverables/fmwk/pub_del_D14.1.a_ec_wp14.1_V4_final.pdf)
- Lia Borthwick: Towards an Open Architecture for European eGovernment Identity Management (http://istrg.som.surrey.ac.uk/projects/guide/files/eChallenges_2004_Paper.doc)
- APES D 4: General report of the legal issues (2003, https://www.cosic.esat.kuleuven.ac.be/apes/docs/APES_d4.doc.gz)
- Alfred J. Menezes/ Paul C van Oorschot/ Scott A. Vanstone, Handbook of applied cryptography, CRC Press, 1996, downloadable at: http://www.cacr.math.uwaterloo.ca/hac/
- ISO/IEC 1st WD 24742: 2005-01-10
- ISO/IEC 21827: 2002-10-01
- ISO/IEC 11770-2: 1996-04-15
- ISO/IEC 15945: 2002-02-01
- ISO IS 15408
- ISO/IEC 15408-2:1999
- ISO/IEC 2nd FCD 18033-2: 2004-12-06
- ISO/IEC 9798-6:2005(E)
- FIDIS D 3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems"
- Regulating a European eID – A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID for the Porvoo e-ID Group by Thomas Myhr
- The Laws of Identity, Kim Cameron, Architect of Identity, Microsoft (http://www.identityblog.com)
- The definitions list of the Dutch government, available through https://www.pkioverheid.nl
- Austrian E-Government Act, Federal Act on Provisions Facilitating Electronic Communications with Public Bodies, Austrian Federal Law Gazette, Part I, No. 10/2004
- Stephen T. Kent / Lynette I. Millett: Who Goes There? Authentication Through the Lens of Privacy. The National Academies Press, 2003, downloadable at http://books.nap.edu/html/whogoes/index.html
- Liberty Technical Glossary, version 1.4 – Liberty Alliance Project
- Lexicon of the Center for Internet Society at Harvard Law School, http://www.identitygang.org/Lexicon
- The SAML glossary 2.0-os available at http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

- The identity management related terms defined by the Open Privacy Initiative, cf. http://www.openprivacy.org/opd.shtml
- http://www.faqs.org/rfcs/rfc2828.html
- http://www.itu.int/ITU-T/studygroups/com17/def005.doc
- Identity concepts and definitions of the Identity management technology thread of the Burton group, Dan Blum
- Identification and Authentication Fundamentals, Roger Clarke
- Privacy and Security, TU Dresden, Dept. of computer science, Institute of system architecture, Anon Terminology Paper, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

This document is intended as a consultation paper, and has not yet undergone a formal review by the Commission. The Modinis[IDM] Study team is keenly aware that community consensus around the definitions is a prerequisite for success. Therefore, we hereby cordially invite all interested parties to contribute their thoughts and feedback on the terminology paper, so that it may be further refined. Any comments are welcome at modinis-idm@esat.kuleuven.be.

For more information about the Modinis[IDM] Study and a continuously updated version of the Modinis[IDM] Terminology Paper, we refer to our web site: https://www.cosic.esat.kuleuven.be/modinis-idm.

2. Table of Contents

3. Scope of the terminology document

During the first Modinis[IDM] Workshop of 4 May 2005 in Leuven, one of the first problems identified as a barrier to the development of interoperable IDM systems in eGovernment is the lack of a common conceptual framework. This was identified by the Modinis[IDM] Study Team as a key issue that needs to be resolved; a position which was subsequently supported by the eEurope eGovernment subgroup – Ad hoc group on Identification and Authentication during its session in Brussels on 30 June 2005.

Part of the conceptual framework – which includes every aspect of the IDM infrastructure – is made up of the terminological framework: the definitions of all concepts of the infrastructure. The lack of a common understanding of even the most prevalent IDM notions constitutes a meta-problem which obstructs a constructive dialogue on the problem of interoperable identity management as a whole. There is no common agreement on the definition of essential concepts such as identity, entity, attribute, delegation, or even entity authentication and identity management.

The current definitions vary widely, since they reflect a complete different point of view on such issues as the use of unique identifiers, who should manage identities and the scope of the definitions. As a practical example, it is nearly impossible to discuss privacy protection questions when there is no consensus about the attributes that define an entity, or if an entity can be something other than a natural person (e.g., a legal person, or even an object such as a computer system, where privacy concerns would not apply).

This paper deals with this issue by attempting to propose a series of neutral and internally consistent definitions of such IDM concepts, thus creating eGovernment IDM ontology. The definitions are based on the preparatory work done through other European projects and initiatives (such as FIDIS, PRIME and GUIDE), amended and completed by inputs from several eGovernment initiatives (such as the aforementioned subgroup, IDABC and of course the Modinis[IDM] Study itself).

The quality of any ontology depends on three characteristics: coverage (level of completeness), consensus (agreed upon), and accessibility (ease of use). It is thus important to note that this is a consultation paper, intended to draw criticism and generate constructive feedback. As such, it should be considered provisional in its entirety.

4. Terminology

This section presents a variety of definitions regarding identity management. Beyond a short definition, further explanatory comments according to the term defined are presented.
The terms provided in this section aim to propose a shared vocabulary for common IDM terminology, taking into account the specific eGovernment IDM context. It is intended to provide all stakeholders with a common terminology, in order to facilitate further debate in this field and contribute to the further growth of a more general IDM conceptualisation. Thus, the definitions are ultimately intended to function as an enabler for the creation of a pan-European IDM architecture.

4.1 Access control

Definition: ***Access control*** *is the protection of resources with technical, regulatory and organizational measures against access or use by unauthorized entities.*

4.2 Anonymity

Definition: ***Anonymity*** *refers to the quality or state of being not identifiable within the set of all possible entities that could cause an action and that might be addressed.*

In this state, the involvement of an entity in a given process is concealed, so that a given action can not be attributed to a specific entity.
The set in which an entity is anonymous typically varies in time and decreases in size as digital systems do not "forget".

4.3 Assertion

Definition: an ***assertion*** *is synonymous with a credential.*

4.4 Attribute

Definition: An ***attribute*** *is a distinct, measurable, physical or abstract named property belonging to an entity.*

An attribute has a type and a value. It is any piece of information about an entity, which does not necessarily uniquely distinguish the entity from any other entity in a given context. Attributes include the characteristics of an entity.
An entity has a finite, but unlimited number of attributes.

4.5 Authentication

Definition: ***Authentication*** *is the corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence.*

Authentication may be used during any IDM process. Authentication serves to demonstrate the integrity (i.e., equivalence to a corresponding reality) and origin (i.e., the source) of what is being pretended (the claimed information). The security and reliability of authentication mechanisms may vary dependant on the desired authentication level. The stronger the authentication, the higher the confidence that an entity corresponds with the claimed set of attributes.

Authentication is typically subdivided into two separate classes: data authentication and entity authentication. For this reason, autonomous use of the term "authentication" (without specifying the type of authentication) should be avoided, as it is subject to (mis)interpretation.

Authentication can be unilateral or mutual. Unilateral authentication provides assurance of the identity of only one entity, where mutual authentication provides assurance of the identities of both entities.

4.5.1 Data authentication

Definition: ***Data authentication*** *is the corroboration that the origin and integrity of data is as claimed.*

Data authentication is a technical process which (in an IDM context) serves to verify that any claimed attribute corresponds to the actual attribute held by an entity.

It is worth noting that data authentication verifies origin and integrity (i.e., the correspondence of a claimed attribute to an attribute that was issued to a specific entity), but not necessarily truth (i.e., the factual correctness of the claimed attribute). E.g., an authentication token containing incorrect data (e.g., an incorrect name) could be used to authenticate data which is factually wrong. Data authentication protects against manipulation (insertion, substitution or deletion) by unauthorised parties; not against e.g., incorrect issuance of credentials or tokens.

4.5.2 Entity authentication

Definition: ***Entity authentication*** *is the corroboration of the claimed identity of an entity and a set of its observed attributes.*

As a part of entity authentication, entities can be identified by factors: knowledge (e.g., password), possession (e.g., token), a personal characteristic (biometrics), location (e.g., network address or phone number), etc., or by a combination of these factors. A typical example of a two-factor authentication mechanism consists of the combination of password and fingerprint authentication.

The specific case of biometrics can be considered a variation of possession (e.g., fingerprint authentication demonstrates the possession of the required fingertip). As the only difference between biometry and other forms of possession is the decreased likelihood of accidental loss of the identifying element, it does not necessitate specific attention at this point.

Entity authentication can be unilateral or mutual. Unilateral authentication provides assurance of the identity of only one entity. Mutual authentication provides assurance of the identities of both entities.

4.6 Authorisation

Definition: ***Authorisation*** *refers to*

(1) the permission of an authenticated ***entity*** *to perform a defined action or to use a defined service/resource;*

(2) the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

Usually, authorisation is in the context of authentication. Permission is granted or denied based on the result of data or entity authentication, and on the allowed activities, as defined within the system. Once an entity is authenticated, it may be authorized to perform different types of access, each of which is referred to as a role.

4.7 Characteristic

Definition: A ***characteristic*** *of an entity is an attribute specific to a particular context.*

A characteristic does not need to uniquely identify an entity. Characteristics indicate an entity's capacity, function, and qualification, etc.

Examples:
- the prime minister of a particular country or a prime minister in a group of prime ministers;
- the Belgian national registry number of a citizen in Belgium or the same number determining a part of a computer device.

While a characteristic is a single attribute, in practice it often implies a set of other attributes, which may or may not be included in the system. E.g., the characteristic of being a doctor implies adulthood and the completion of a certain education.

4.8 Confidentiality

Definition: ***Confidentiality*** *refers to the state of keeping the content of information secret from all entities but those authorised to have access to it.*

4.9 Context

Definition: a ***context*** *is a sphere of activity, a geographic region, a communication platform, an application, a logical or physical domain.*

Practically, a context is only relevant in an interaction.

4.10 Corroboration

Definition: ***Corroboration*** *is the confirmation by provision of sufficient evidence and examination thereof that specified requirements have been fulfilled.*

The term "verification" is often used as a synonym of corroboration. However, this term is somewhat more dubious, as it is also occasionally used as a synonym of authentication (either entity or data authentication). For this reason, "corroboration" should be preferred over "verification".

"Sufficient evidence" is determined by the Identity Management System. It is possible that the amount of evidence required is (virtually) non-existent or holds (virtually) no legal value, e.g., a simple set of claims (e.g., claiming to have a certain name or address).

4.11 Credential

Definition: A ***credential*** *is a piece of information attesting to the integrity of certain stated facts.*

Credentials are primarily used in the process of entity authentication, and are then often incorporated in an authentication token, e.g., a smart card, bank card, mobile phone, etc.

Note that credentials are not always integrated into a token: in certain systems, a password might function as a credential, despite the lack of a medium carrying the information. Certificates are a common type of credential in a PKI system, where they often take the form of so-called *attribute certificates*: a credential attesting to the integrity of one or more attribute values with identification information about the corresponding entity.

Credentials are typically revocable.

4.12 Delegation

Definition: ***Delegation*** *is the process in which an identified entity issues a mandate to another identified entity.*

From a legal perspective, the concept of delegation usually implies acceptance by the receiving identified entity. In a technical context, acceptance is usually unnecessary.

A mandate can be used to delegate authorizations of one identified entity to another.

4.13 Digital Identity

Definition: A ***digital identity*** *is a partial identity in an electronic form.*

For any given entity, there will typically exist many digital identities which may be unique or non-unique. A digital identity can be created on the fly when a particular identity transaction is desired.

A digital identity is, by definition, a subset of the identity, and can in effect be considered a manifestation of an entity's presence in an electronic IDM system (i.e., it is the subset of attributes belonging to an entity that is accessible through a specific IDM system).

4.14 Enrolment

*Definition: An **enrolment** is synonymous with a **registration**.*

4.15 Entity

*Definition: An **entity** is anyone (natural or legal person) or anything that shall be characterised through the measurement of its attributes.*

The choice was made to provisionally keep this definition open to any type of person (including legal persons, to facilitate e.g., eProcurement), but also to any other type of entity, such as objects (e.g., computers or other forms of machinery), digital resources or processes (e.g., programmes), as this allows abstraction to the largest common element and thus offers the largest number of applications.

In order for its existence to be acknowledged, an entity needs to have at leas one unique identity.

4.16 Federated Identity

*Definition: A **federated identity** is a credential of an entity that links an entity's partial identity from one context to a partial identity from another context.*

4.17 Identifiable Entity

*Definition: An **identifiable entity** is an entity whose identity can be established.*

4.18 Identification

*Definition: **Identification** is the process of using claimed or observed attributes of an entity to deduce who the entity is.*

The term "identification" is also referred to as entity authentication. The identification of an entity within a certain context enables another entity to distinguish between the entities it interacts with.

4.19 Identified entity

*Definition: An **identified entity** is an identifiable entity the identity of which has been corroborated.*

The term "identified entity" is also referred to as an "authenticated identity."

As indicated below, corroboration entails that a given element has been proven to the extent required by the Identity Management System. As such, there are no fixed rules or criteria to meet before an entity can be considered identified. The only criterion is the acceptance of the identification by the IMS.

4.20 Identifier

*Definition: An **identifier** is an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context.*

For the sake of clarity, identifiers consisting of one attribute are also characteristics; they distinguish an entity from other entities.

An entity may have multiple distinct identifiers referring to it. Identifiers uniquely identify an entity, while characteristics do not need to. However, it should be noted that identifiers can consist of a combination of attributes, whereas characteristics are always one single attribute.

4.21 Identity

*Definition: The **identity** of an entity is the dynamic collection of all of the entity's attributes. An entity has only one identity.*

An entity has only one identity, consisting of a number of attributes that need not necessarily be unique for that entity, but which are nonetheless useful when attempting to distinguish several entities. Common examples of such attributes include name, date and place of birth, address, the identity of parents, etc.

As such, the identity is a fluid and evolving philosophical concept, rather than a practical one: as it is impossible for any one IDM system to gather all attributes of any specific entity, IDM systems must focus on a specific subset of relevant attributes.

As a rule of thumb, when people refer to **the** identity of an entity, they are referring to the essence of the entity as defined above. In contrast, when they refer to **an** identity of an entity, they are referring to the concept of **partial** identity, as defined below.

This brings us to the following concepts.

4.22 Identity management (IDM)

*Definition: **Identity management** is the managing of partial identities of entities, i.e., definition, designation and administration of identity attributes as well as choice of the partial identity to be (re-) used in a specific context.*

4.23 Identity management application

*Definition: An **identity management application** is a tool used by an entity to manage partial identities.*

In general, the identity management application is used to manage partial identities, e.g., for their creation, updating, revocation, etc.

4.24 Identity management system (IMS)

*Definition: An **identity management system** is the organisational and technical infrastructure used for the definition, designation and administration of identity attributes.*

4.25 Mandate

*Definition: A **mandate** (or **proxy**) is a revocable role or a set of revocable roles which refer(s) to one or more permissions granted by an identified entity to another identified entity to perform well-defined actions with legal consequences in the name and for the account of the former.*

Mandates are a type of characteristic, and thus also an attribute. Mandates (or proxies) must be revocable. E.g., the power of attorney or a parent's authority over its underage child.

4.26 Non-repudiation of origin

*Definition: **Non-repudiation of origin** is the ability to prevent an acting entity from denying at a later stage that it performed that specific action.*

4.27 Nym

*Definition: A **nym** is synonymous with a **pseudonym**.*

4.28 Partial Identity

*Definition: A **partial identity** is a certain subset of one or more attributes that does not necessarily uniquely identify the entity.*

While an entity has only one identity, it may have many partial identities. Partial identities are often simply referred to as "identities", which may lead to confusion when they refer to a single entity. For this reason, the term "partial identity" should be preferred.

4.29 Permission

*Definition: **Permission** describes the privileges granted to an authenticated entity with respect to low-level operations that may be performed on some resource (e.g., read, write, delete, execute, create…).*

Permissions are also referred to as "access rights."

4.30 Persona

*Definition: A **persona** is a pre-existing digital identity that an entity can select and use to represent itself in a given context.*

A persona is something put forward by an entity, but how it is perceived, recognized, accepted, rejected, trusted, used, etc. by another entity cannot be specified or in any way implied. It is often used when the set of credentials of the entity represents a role or has a virtual character animated by the entity.

4.31 Personally identifiable information

*Definition: **Personally identifiable information** is any data that identifies or refers to a particular natural or legal person.*

4.32 Principal

*Definition: A **principal** is synonymous with an identifiable entity.*

4.33 Privacy

*Definition: **Privacy** is the right of an entity – in this context usually a natural person – to decide for itself when and on what terms its attributes should be revealed.*

Privacy can alternatively be described as the freedom of a natural person to sustain a "personal space", free from interference by other entities.

In an IDM context, privacy is mostly used as a synonym of "informational privacy", i.e., the interest of a natural person to control, or at least significantly influence the handling of data about themselves, also taking into account the nature of the applicable attributes and the entity in charge of data management.

4.34 Privacy enhancing technology (PET)

*Definition: A **privacy enhancing technology** is hardware or software which increases the ability of a natural person to actively influence the availability of information about and exposure of itself.*

4.35 Profile

*Definition: A **profile** of an entity or a group of entities is an organized set of attributes that characterizes the specific properties of that entity or entities within a given context for a specific purpose.*

4.36 Profiling

*Definition: **Profiling** is the practice of collecting and analysing data related to an entity with the aim of creating its profile.*

4.37 Proxy

*Definition: A **proxy** is synonymous with a **mandate**.*

4.38 Pseudonym

*Definition: A **Pseudonym** (syn.: **nym**) is an arbitrary identifier of an identifiable entity, by which a certain action can be linked to this specific entity. The entity that may be identified by the pseudonym is the holder of the pseudonym.*

A pseudonym is typically a fictitious name that can refer to an entity without using any of the entity's identifiers. In effect, the pseudonym is an additional attribute of a given entity's identity, which allows it to form a set of partial identities which can not necessarily be easily traced to the originating entity.
As identifiers, pseudonyms are context-bound, and one pseudonym is not necessarily valid across multiple identity management systems.
An entity is pseudonymous if it relies on a pseudonym as identifier.

4.39 Registration

*Definition: The **registration** of an entity is the process in which the entity is identified and/or other attributes are corroborated. As a result of the registration, a partial identity is assigned to the entity for a certain context.*

In other words, the registration of an entity is the process of linking a (partial) identity to the identity of an entity, by corroborating a specific set of attributes, which do not necessarily need to include identifiers.

Successful completion of the registration procedures results in the granting of a means (e.g., a credential) by which the entity can be authenticated in the future.

Quality assurance criteria (with various degrees of liability attached) can be imposed on the registration process.

4.40 Resource

*Definition: a **resource** is either data related to some identity or identifiers, or a service acting on behalf of some identity or group of identities.*

The set of technical, regulatory and organizational measures intended to protect system resources against access by unauthorized entities.

4.41 Role

*Definition: A **role** is a set of one or more authorisations related to a specific application or service.*

4.42 Token

*Definition: A **token** is any hardware or software that contains credentials related to attributes.*

Tokens may take any form, ranging from a digital data set to smart cards or mobile phones.

Tokens can be used for both data/entity authentication (**authentication tokens**) and authorisation purposes (**authorisation tokens**).

4.43 Trust

*Definition: **Trust** is a quality of a relationship between two or more entities, in which an entity assumes that another entity in the relationship will behave in a fashion agreed beforehand, and in which the first entity is willing to act on this assumption.*

Whether or not to trust depends on a natural person's decision. It is possible, but not necessary that several entities trust each other mutually in a certain context. Trust decisions of legal persons depend on the decisions made by the legal person's responsible natural persons.

Trust may be limited to one or more specific functions, and may depend on the fulfilment of one or more requirements.

4.44 Trusted third party (TTP)

*Definition: A **trusted third party** is an entity trusted by multiple other entities within a specific context and which is alien to their internal relationship.*

4.45 Unique identity

*Definition: A **unique identity** is a partial identity in which at least a part of the attributes are identifiers.*

Since at least some of the attributes (or combinations thereof) are identifiers, the entity can be uniquely identified through the unique identity within a certain context. A unique identity is an identifier such as a unique number or any set of attributes that allows one to determine precisely who or what the entity is.

Prepared by:

The Modinis IDM Study Team
B-3000 Leuven, Belgium

https://www.cosic.esat.kuleuven.ac.be/modinis-idm/

Lead contractor:
K.U.Leuven Research & Development, Belgium

Project manager: prof. Bart Preneel

http://www.esat.kuleuven.be/cosic

Subproject manager: prof. Jos Dumortier

http://www.icri.be

Subcontractor:

Secure Information Technology Center, Austria (A-SIT)

Director: prof. Reinhard Posch

http://www.a-sit.at

Subcontractor:

Lawfort – ICT Law Department, Belgium

Head: prof. Jos Dumortier

http://www.lawfort.be

For further information about the eGovernment Unit

European Commission
Information Society and Media Directorate-General
eGovernment Unit

Tel (32-2) 299 02 45
Fax (32-2) 299 41 14

E-mail EC-egovernment-research@cec.eu.int
Website europa.eu.int/egovernment_research

ANEXO B: ENTREVISTA COM DR. MÁRIO AUGUSTO M. F. CORREIA COSTA, CAIXA GERAL DE DEPÓSITOS

Marco Pereirinha: Qual a melhor forma para efectuar pagamentos de pequenas quantias no contexto dos municípios?

Mário Costa: A melhor maneira para efectuar pagamentos de pequenas quantias é, os pagamentos designados no sistema bancário como de "baixo valor".

MP: Será viável o pagamento de serviços com um cartão não bancário?

MC: É viável. São os cartões pré pagos. São cartões semelhantes aos bancários PMB (porta moedas Multibanco). Enquanto nestes eram possíveis os recarregamentos, já os pré pagos são como os cartões dos telefones. O cartão custa X e os portadores gastam até aquele limite. A vantagem é que não obriga a existência de conta bancária, no entanto o cliente avança com o dinheiro. Tem um efeito psicológico negativo.

MP: É previsível a adopção de um sistema semelhante ao da via verde, no pagamento de serviços municipais?

MC: Previsível, não sei, mas possível é.

MP: Qual seria o procedimento?

MC: O sistema é em tudo semelhante à adesão a um TPA (terminal de pagamento automático). A diferença reside no facto de nunca nenhuma transacção ser feita online. As transacções são armazenadas e posteriormente o ficheiro é enviado à SIBS. As contas dos utilizadores são debitadas e creditadas as dos fornecedores. Nestes casos é sempre necessário o recurso a uma conta bancária. A Via Verde pressupõe a existência de um identificador ao qual está relacionada uma matrícula, um modelo de carro e uma conta. Para estas situações penso que a existência de um leitor do chip do cartão resolveria o problema.

ANEXO C: ENTREVISTA COM DRA. ROSSANA FERNANDES CHEFE DE SECÇÃO NA CÂMARA MUNICIPAL DE AVEIRO

Marco Pereirinha: Qual a importância dos sistemas de identificação?

Rossana Fernandes: São importantes tanto a nível interno como a nível externo:

- A nível da instituição para controlo dos funcionário, por exemplo na assiduidade, e para que possam ser identificados com facilidade pelos utentes.
- A nível de utente para facilitar todos os processos. Havendo um sistema electrónico de identificação, o utente deixará de ter que trazer consigo a panóplia de cartões de identificação que hoje são necessários.

MP. Que potencial e riscos estão associados com a adopção de meios de identificação de munícipes?

RF: Será mais fácil para o funcionário resolver cada uma das situações que surgirem pois todos os assuntos relacionados com o utente estarão interligados. De um só terminal se poderão visualizar todos os processos e responder a questões relacionadas com esses processos sem a pessoa ter que se deslocar e sem que o funcionário seja "acusado" de burocrata e de querer passar o trabalho para outro colega. Gabinete de Atendimento ao Utente (Balcão único de atendimento).

Penso, no entanto, que existe sempre o risco de fraude. Em todos os tipos de sistema ela existe, basta haver um geniozinho que a isso se dedique.

MP. Em que é que se suporta o actual relacionamento entre a Administração Pública e os munícipes?

RF: Neste momento, na Câmara Municipal de Aveiro, existe um sistema de gestão de documentação que não resolve todos os problemas, pois vejo com

frequência colegas a telefonarem-se para perguntar por alguns processos ou utentes andarem de sector em sector para saberem dos vários processos que têm. O sistema funciona mal.

MP. Como é validada a identificação do munícipe?

RF: Os utentes têm sempre que se identificar com vários documento, nomeadamente, o bilhete de identidade, contribuinte, comprovativo de morada.

MP. Qual a percepção de uma gestão sistemática da identificação do cidadão transversal ao município?

RF: Torna-se urgente um sistema de gestão de informação que consiga cruzar todas as informações existentes para facilitar a vida tanto ao utente como ao funcionário.

MP. Como poder ser considerado e se fará sentido o envolvimento do sector privado?

RF: Em imensos aspectos já existe o envolvimento das instituições públicas com sector privado. Desde empresas fornecedoras de bens e serviços até empresas que complementam os serviços prestados pela Câmara.

ANEXO D: ENTREVISTA COM ENG. PAULO MARQUES, DIRECTOR TÉCNICO DA EMPRESA VIA VERDE PORTUGAL – GESTÃO DE SISTEMAS ELECTRÓNICOS DE COBRANÇA, SA

Marco Pereirinha: Que serviços disponibiliza a Via Verde?

Paulo Marques: A Via Verde presta serviços de gestão de sistemas electrónicos de cobrança, utilizando infra-estruturas aplicáveis a veículos automóveis. Nomeadamente, o pagamento de portagens nas auto-estradas, o pagamento nos postos de abastecimento de combustíveis da Galp, o controlo nos acessos a bairros históricos, o pagamento de estacionamento em parques subterrâneos e, durante o 2º semestre de 2006, será disponibilizado o pagamento de estacionamento em parques de rua.

MP: Como são realizadas as transacções financeiras?

PM: A Via Verde trabalha em estreitas ligações com a SIBS e a rede bancária, disponibilizando aos seus clientes 3 tipos de pagamentos: as transacções de baixo valor, os pré pagos e os débitos directos.

MP: Poderá conceptualizar sinteticamente cada um deles?

PM: O pagamento através das designadas transacções de baixo valor é feito por intermédio do *clearing* financeiro SIBS. Este método é utilizador, por exemplo, nas portagens. No caso do sistema de portagens fechado, onde o preço final depende da classe do veículo e do local de entrada, é gerado um *ticket* na barreira de entrada sendo memorizado no dispositivo OBU (*on board unit*), contendo as informações relativas à portagem de entrada, à via de entrada e à hora da entrada. Na barreira de saída, uma antena lê as informações armazenadas no *ticket*, registando o evento numa base de dados alojada no recinto da portagem. Durante o dia são realizadas diversas actualizações onde são emitidas para o sistema central todas os eventos ocorridos até aquele momento. Estes eventos são analisados de forma a rastrear tentativas fraudulentas. Posteriormente os dados do identificador e

valores correspondestes aos eventos são enviados para a SIBS. Através do relacionamento nas suas bases de dados, a SIBS consegue transformar uma transacção "assignada" a um identificador, para uma transacção "assignada" a um cartão Multibanco, de forma a creditar a Via Verde. O sistema Via Verde é o garante da segurança da transacção, que entre outros sistemas de segurança anti-fraude, assegura que não há identificadores repetidos.

Os pré pagos serão utilizados, por exemplo, no estacionamento de rua. Os clientes efectuam um carregamento nas caixas ATM, como no caso dos telemóveis, usando o protocolo *realtime* que existe com a SIBS. Frequentemente são efectuadas actualizações, em método *broadcast*, para todas as antenas espalhadas pela cidade. Quando o cliente passa junto duma antena, o seu OBU é actualizado com o novo saldo. Assim que o cliente estaciona na rua, este selecciona a tarifa (não o valor, mas uma referência abstracta que identifica a zona) e activa o OBU. Não precisa de nenhuma antena perto. Funciona como se tivesse um *ticket* impresso, colocado no *tablier* do automóvel. Com uma antena especial, os fiscais sabem se o OBU está ou não activado, há quanto tempo está activado e o saldo ainda disponível. Quando o cliente chega ao carro desactiva o dispositivo e arranca normalmente. Assim que o automóvel passe por uma antena, além da recolha do detalhe das transacções de estacionamento efectuadas , há uma sincronização entre o saldo no OBU e o saldo nos sistemas centrais. Desta forma garante-se um controlo dos saldos "*on board account*", pois a informação está armazenada no dispositivo e, um controlo "*off board account*" em que o saldo dos OBUs está armazenado nos servidores centrais.

Por fim, o débito directo é usado como uma forma de efectuar os carregamentos de pré pagos, ou seja, o cliente define um valor a ser creditado no seu OBU que permitirá ir descontando os custos dos serviços prestados pela Via Verde. A diferença reside no facto em que uma vez gasto o valor creditado, é automaticamente realizada uma operação de débito directo junto do banco do cliente, de forma a creditar o OBU.